Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von:	Dipl.-Ing. Tobias Ständer
aus (Geburtsort):	Kassel

eingereicht am:	19.08.2010
mündliche Prüfung am:	10.12.2010
Referenten:	Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder
	Prof. Dr.-Ing. Bernd Bertsche

2011

Vorwort

Die vorliegende Arbeit entstand auf Basis meiner Tätigkeiten am Institut für Verkehrssicherheit und Automatisierungstechnik der TU Braunschweig in den Jahren 2004-2009. An dieser Stelle möchte ich mich bei allen bedanken, die mich bei der Fertigstellung dieser Arbeit unterstützt haben.
Dem Institutsleiter, Herrn Prof. Dr.-Ing. Dr. h.c. mult Eckehard Schnieder, danke ich gleichermaßen für seine langjährige Unterstützung, für zahlreiche wissenschaftliche Diskussionen, für konstruktive Hinweise und seine sehr persönliche Begleitung.
Desweiteren danke ich Herrn Prof. Dr.-Ing. Bernd Bertsche, Leiter des Instituts für Maschinenelemente der Universität Stuttgart, für sein Interesse an meiner Arbeit und die Übernahme des Korreferats. Ebenso möchte ich mich bei Herrn Prof. Dr.-Ing. Ferit Küçükay, Leiter des Instituts für Fahrzeugtechnik der TU Braunschweig, für die Übernahme des Vorsitzes der Prüfungskommission bedanken.
Ein herzlicher Dank geht auch an meine ehemaligen Kollegen des Instituts, in dessen Kreis ich sowohl die fachlichen Diskussionen als auch die freundschaftliche Zusammenarbeit sehr geschätzt habe. Mein besonderer Dank für wertvolle Fachgespräche und ebenso wertvolles Korrekturlesen gilt hierbei Herrn Dipl-Ing. Daniel Beisel und Dipl.-Math. Tobias Lück. Desweiteren möchte ich mich bei Frau Regine Stegemann und dem gesamten Team des Geschäftszimmers bedanken, die mir über meine gesamte Institutszeit, und darüber hinaus, mit Rat und Tat beseite gestanden und mich nicht nur beim Korrekturlesen unterstützt haben.
Natürlich danke ich auch meinen Eltern die mir mein Studium an der TU Braunschweig ermöglicht und so den Grundstein für die erfolgreiche Promotion gelegt haben und mich auf meinem Lebensweg bis heute immer unterstützt haben.
Widmen möchte diese Arbeit meiner Frau Nina und unseren Töchtern Mia und Lina. Danke für Eure Unterstützung, Eure Geduld und die Ruhe, die Ihr mir insbesondere im letzten Jahr Wochenende für Wochenende zuteil habt kommen lassen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abstract

The development of future electrical, electronic and programmable electronic systems (E/E/PE-systems) in motor vehicles is expected to be more and more influenced in the coming years by the standard *ISO 26262*, which is currently available as a Draft International Standard. This standard provides requirements for the entire safety lifecycle including the *concept phase*, the *product development*, the *start of production* and the *operation*.

One essential part of the concept phase consists in performing a *hazard analysis* and *risk assessment* (HA&RA). The objective of this phase is to identify and categorize the hazards emanating from the item to be developed in terms of their risk potential.

Different methods are recommended in ISO 26262 (e.g. FMEA, checklists etc.) to identify these hazards. Once the potential hazards have been identified, these can be evaluated in terms of the risk posed by them, using the approach recommended in ISO 26262 to determine an *Automotive Safety Integrity Level* (ASIL). This assessment is largely based on *subjective* – mostly conservative – *estimations* (pronounced by experts) of the ASIL-characterizing parameters: *probability of exposure* (E), *severity* (S) and *controllability* (C). This is the reason why safety related systems are often oversized.

In this thesis a method is described thanks to which the aforementioned subjective evaluations can be reduced by the *simulation* and *analysis* of *Petri net models*. After an intensive discussion and *conceptual analysis* of the ASIL-determining parameters (E, S and C), the scope of the me-thod is limited to the model-based objectification of the probability of exposure in a relevant op-erational situation.

The developed Petri net models, initially supposed to be obeying a *deterministic behavior*, are used to determine the probability of exposure in functionally relevant scenarios and to validate the gleaned values and the correctness of the model against the results of an event tree analysis (ETA). Moreover, the determined probability of exposure is validated with respect to its plau-sibility by comparing it with the result of an assessment carried out conventionally under the terms of ISO 26262.

In the following it is assumed that a large number of factors characterizing real driving situations (e.g. rain, fog, etc.) are following a *stochastic behavior*. In this case, the analytical calculation of the probability of exposure by means of an ETA is limited and the determined values‘ plausibility can only be validated by comparison

with the results of a conventional estimation.
Depending on the subjective assessment of an expert risk analyst the developed method logi-cally can lead to both, an *ASIL-reduction*, and thus to a reduction of the development costs (e.g. single-channel implementation instead of two-channel implementation), as well as an *ASIL-increase*, and thus to related additional work and expense in the development (e.g. resulting higher test coverage).
In both cases due to its structured model-based approach, the presented EmMORI-method (Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262) can *back up an ASIL-classification in front of decision-makers.* Thus the *practical usefulness* of the method is given.

Zusammenfassung

Die Entwicklung zukünftiger elektrischer, elektronischer und programmierbarer elektronischer Systeme (E/E/PE-Systeme) in Kraftfahrzeugen wird in den nächsten Jahren voraussichtlich immer mehr von der, derzeit als Draft International Standard vorliegenden Norm, *ISO 26262* beeinflusst. Diese Norm stellt Anforderungen an den gesamten Sicherheitslebenszyklus von der *Konzeptphase* über die *Systementwicklung* bis hin zum *Produktionsstart*.
Ein wesentlicher Bestandteil der Konzeptphase ist die *Gefährdungsidentifikation und Risikobewertung*. Ziel dieser Phase ist es potenziell vom zu entwickelnden System ausgehende Gefährdungen zu identifizieren und hinsichtlich ihres Risikopotenzials zu bewerten. Zur Identifikation der Gefährdungen werden in ISO 26262 unterschiedliche Methoden (z.B. FMEA, Checklisten etc.) vorgeschlagen. Sind potenzielle Gefährdungen erkannt, können diese mittels des in ISO 26262 beschriebenen Ansatzes zur Ableitung eines Automotive Safety Integrity Levels (ASIL) hinsichtlich des von ihnen ausgehenden Risikos bewertet werden. Diese Bewertung basiert in hohem Maße auf der *subjektiven* – meist konservativen – *(Experten-)Einschätzung* der den ASIL charakterisierenden Parameter *Expositionswahrscheinlichkeit (E), Schadensausmaß (S) und Kontrollierbarkeit (C)*, weswegen Sicherungsfunktionen häufig überdimensioniert werden.
In der vorliegenden Arbeit wird eine Methode beschrieben, welche diese subjektiven Einflüsse durch *Simulation und Analyse* von *Petrinetz-Modellen* reduzieren kann. Hierbei wird sich nach intensiver Diskussion und *begrifflicher Analyse* der die ASIL-Einstufung bestimmenden Faktoren (E, S und C) auf die modellbasierte Objektivierung der Expositionswahrscheinlichkeit in einem relevanten Fahrszenario beschränkt. Die Methode und die Struktur der, wie zunächst angenommen, einem *deterministischem Verhalten* folgenden Modelle werden im Sinne einer Anwendbarkeitsstudie exemplarisch zur Bestimmung der Expositionswahrscheinlichkeit in funktionsrelevanten Szenarien angewendet. Die Ergebnisse werden mittels einer Ereignisbaum-Analyse (ETA) validiert und zur Plausibilisierung mit den Ergebnissen einer herkömmlich durchgeführten Einschätzung nach ISO 26262 verglichen.
Im Folgenden wird davon ausgegangen, dass eine Vielzahl von die realen Fahrsituationen charakterisierenden Faktoren (z.B. Regen, Nebel etc.) einem *stochastischem Verhalten* folgen. In diesem Fall stößt die analytische Berechnung der Expositionswahrscheinlichkeit mittels einer ETA an ihre Grenzen, weswegen deren Plausibilität

nur noch durch den Vergleich mit herkömmlichen Schätzungen überprüft werden kann.
Die entwickelte Methode kann nachvollziehbarerweise in Abhängigkeit von den subjektiven Einschätzungen eines Referenz-Risikoanalysten sowohl zu einer *ASIL-Reduktion*, und damit einhergehenden Einsparpotenzialen hinsichtlich der Entwicklungskosten (z.B. einkanalige statt zweikanalige Umsetzung), als auch zu einer *ASIL-Erhöhung*, und damit verbundenem Mehraufwand bei der Entwicklung (z.B. höhere Testabdeckung gefordert), führen.
In beiden Fällen kann die EmMORI (Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262) genannte Methode aufgrund ihres strukturierten modellbasierten Ansatzes helfen die *ASIL-Einstufung* gegenüber *Entscheidungsträgern zu vertreten*, wodurch die praktische Verwertbarkeit der Methode gegeben ist.

Kapitel 1

Einleitung und Motivation

Die Entwicklung von technischen Systemen wird sich auch in Zukunft der Herausforderung eines stetigen Komplexitätszuwachses bei gleichzeitig immer kürzeren Entwicklungszyklen und restriktiveren rechtlichen Rahmenbedingungen stellen müssen. In der Automobilbranche werden diese Rahmenbedingungen voraussichtlich in Zukunft immer stärker von der ISO 26262 [ISO26262] [1] geprägt. Diese Norm beschreibt u.a. die Vorgehensweise zur Durchführung einer *Gefährdungsidentifikation und Risikobewertung*[2] für elektronische Fahrzeugsysteme (z.B. Fahrerassistenzsysteme), welche neu am Markt positioniert werden sollen. Schon heute hat diese Methode bei Zulieferern und OEMs Einzug in die Entwicklungsprozesse gehalten; dies obwohl der Normungsprozess der ISO 26262 noch nicht abgeschlossen ist und daher aus produkthaftungsrechtlichen Gründen noch immer die Sicherheitsgrundnorm IEC 61508 [IEC61508] anzuwenden ist.
Erste Erfahrungen (s. z.B. [Pau07]) zeigen, dass die in der ISO 26262 beschriebene Risikoanalyse-Methode den Ansprüchen der Automobilbranche zwar wesentlich besser genügt, als es die sehr allgemein gehaltenen Vorgehensbeschreibungen in der IEC 61508 tun, die Risikobewertungen aber immer noch stark von rein subjektiven Abschätzungen des die Analyse durchführenden Personenkreises abhängig sind.

[1] aktuell noch ISO DIS 26262; wird dennoch im Folgenden als ISO 26262 aufgeführt
[2] wird im Folgenden häufig unter dem Begriff *Risikoanalyse* subsummiert

1.1 Ziel dieser Arbeit

Ziel dieser Arbeit ist es eine Methode aufzuzeigen, welche einer kostentreibenden, häufig nicht notwendigen, auf subjektiven Schätzungen basierenden Überdimensionierung der technischen Realisierung von Sicherheitsfunktionen entgegenwirkt.
Die in Abschnitt 1.3.2 exemplarisch aufgezeigten Expertenschätzungen von Aufwänden, Kosteneinflüssen und Zuwandererzahlen verdeutlichen, dass die Ergebnisse von auf Schätzungen basierenden Untersuchungen branchen- und kontextunabhängig in hohem Maße subjektiven Einflüssen unterliegen.
Risikoanalysen und die auf deren Ergebnissen getroffenen Entscheidungen dagegen scheinen in der Gesellschaft den Eindruck zu erwecken objektiv zu sein [Red02] und werden häufig stillschweigend hingenommen.
Eine detailliertere Betrachtung der Inhalte einer *Risikoanalyse* macht jedoch deutlich, dass auch sie stark von subjektiven Meinungen bzw. Interpretationen abhängig ist. Tatsache ist, dass sämtliche Risikoanalyse-Teilschritte sowie die in den einzelnen Phasen zum Einsatz kommenden Beschreibungsmittel und Methoden subjektive Einflüsse mit sich bringen. Diese sind häufig sowohl auf die Notwendigkeit subjektiver Beurteilungen bei der Anwendung von Methoden als auch auf Freiräume für menschliche Befangenheit, also die Projektion eigener Erfahrungen, und allgemeine Schätzungenauigkeiten zurückzuführen [Red02]. Hierin liegt auch begründet, dass es sehr unwahrscheinlich ist, dass zwei unabhängig voneinander agierende Risiko-Analysten, bei gleichen zur Verfügung stehenden Anfangs-Informationen zu den gleichen Analyse-Ergebnissen kommen.
Es wird gleichermaßen deutlich, dass nicht nur bei der Durchführung von Risikoanalysen, sondern auch bei der Interpretation der Ergebnisse ausreichendes Urteilsvermögen erforderlich ist.
So ist es zwar das Ziel einer klassischen Risikoanalyse, potenzielle von technischen Systemen ausgehende Gefährdungen objektiv zu quantifizieren, die Gesellschaft schätzt die Gefahren und Risiken aber in der Regel, basierend auf ihrer Wahrnehmung, ganz anders ein, da für sie jede technische Anwendung abzuwägende Vorteile (Nutzen) und Risiken birgt [Stö99].
Gerade basierend auf dieser unscharfen Wahrnehmung wird oftmals propagiert, dass der Hauptnutzen der Durchführung einer Risikoanalyse nicht in den quantitativen Risikobewertungen liegt, sondern im Zwang, sich überhaupt strukturiert mit dem

von einem System bzw. Prozess ausgehenden Risiko zu beschäftigen.
Redmill weist in [Red02] zudem explizit darauf hin, dass für den Fall, dass die Möglichkeit besteht die Subjektivität zu reduzieren, dies auch getan werden sollte, um die Aussagekraft der Analyse zu erhöhen.
Der kritisierten subjektiven Abschätzung im Rahmen der Risikoanalyse gemäß ISO 26262 soll in dieser Arbeit mittels Simulation und quantitativer Analyse von formalen Modellen mit ausgereiftem mathematischen Hintergrund begegnet werden. Hiermit können Sicherheitsanforderungen objektiv(er), strukturierter und in Einklang mit den in ISO 26262 dokumentierten Anforderungen an die qualitative Risikoanalyse abgeleitet werden. Die so erreichte Vereinigung der qualitativen Elemente der Risikoanalyse nach ISO 26262 mit der objektivierenden quantitativen Analyse formaler Modelle mündet in einer semi-quantitativen bzw. semi-qualitativen Vorgehensweise.
Die Objektivität wird zwangsläufig mit einem nicht unerheblichen Modellierungsaufwand erkauft, welcher zusätzliche Entwicklungskosten verursacht. Diese stehen jedoch in keinem Verhältnis zu den Einsparpotenzialen, welche sich aufgrund einer weniger überdimensionierten technischen Realisierung der Sicherheitsfunktion (z.B. einkanalige statt zweikanalige Struktur) für ein Serienprodukt ergeben und können daher auch gegenüber Entscheidern gut kommuniziert werden.
Die im Folgenden unter dem Akronym EmMORI-Methode („**E**ine **m**odellbasierte **M**ethode zur **O**bjektivierung der **R**isikoanalyse nach **I**SO 26262“) geführte Methode knüpft an das in [Slo06] entwickelte und mittlerweile in DIN IEC 62551 [IEC62551] standardisierte PROFUND-Konzept an, indem ein (Fahr-)**Pro**zess (bzw. das Fahrszenario) modelliert wird, um für eine zu entwickelnde **Fun**ktion (z.B. Fahrerassistenzfunktion) Sicherheits- bzw. Zuverlässigkeitsanforderungen (**D**ependability) abzuleiten.
Als geeignete formale Notation werden nach wissenschaftlich fundierter Analyse (s. Kapitel 4) zur Verfügung stehender Techniken *Petrinetze* gewählt. Diese Wahl lässt sich sowohl vor dem Hintergrund ihres ausgereiften mathematischen Hintergrundes, als auch der Universalität hinsichtlich Simulation und Analyse begründen.
Um die praktische Verwertbarkeit dieses wissenschaftlichen Ansatzes in den Vordergrund zu stellen, wird dem Leser die Anwendung soweit möglich, ohne auf die detaillierten mathematischen Grundlagen der Theorie der Petrinetze und deren Analyseverfahren einzugehen, nahegebracht.

1.2 Entwicklung von Fahrzeugsteuerungssystemen im technologischen Wandel

Die Durchführung von Risikoanalysen und damit ein wesentlicher Schritt auf dem Weg zur Entwicklung von sicheren Fahrerassistenzsystemen ist nicht nur aufgrund der gesetzlichen und normativen Forderungen notwendig, sondern auch vor dem gesellschaftlichen Hintergrund unverzichtbar.
Der Mensch weist gegenüber technischen Systemen eine Vielzahl von Vorteilen auf, z.B. bei der Wahrnehmung oder in der Flexibilität seines Handelns. Dessen ungeachtet sind die ca. 2,23 Mio. Straßenverkehrsunfälle mit ihren ca. 310.000 Verunfallten im Jahr 2009 (nach: [DES09]) in Deutschland zu gut 70% auf fehlerhafte Handlungen des Menschen zurückzuführen.
Fahrerassistenzsysteme (FAS) unterstützen den Fahrzeugführer bei korrekter Funktion bei der Durchführung von Fahraufgaben und tragen damit zur Reduzierung der Unfallhäufigkeit bzw. einer Verbesserung der Verkehrssicherheit bei [SWSB08].
In [DVR07] wird den über die Gesamtlebensdauer des Fahrzeuges wirkenden FAS sogar neben der zeitlich sehr begrenzt einflussnehmenden Verkehrserziehung – in Deutschland ist ein Führerschein innerhalb von zwei Wochen zu erwerben – das größte Potenzial zugesprochen, um Unfallzahlen bzw. -folgen zu mindern.
Die Bandbreite derartiger Assistenzsysteme reicht heute von bloßen Informations- und Warnsystemen über Stabilisierungssysteme bis zu Systemen, die über ihre Aktuatorik und Sensorik aktiv in die Fahrzeugführung (Längs- und Querführung) eingreifen [EWGN08].
Einen umfassenden Überblick über den aktuellen Stand der Technik von Fahrerassistenzsystemen liefert [WHW09].
Eine Fehlfunktion derartiger FAS kann aber auch zu Gefährdungen im Straßenverkehr führen, die ohne das FAS nicht bestünden. Ein anschauliches Beispiel hierfür stellt ein Anti-Blockier-System (ABS) dar, wie es seit Jahren zugelassen und heutzutage in allen Neufahrzeugen serienmäßig integriert ist. Es ist nachvollziehbar, dass ein Ausfall, also ein Rückfall in einen Fahrzeugausstattungszustand ohne ABS, eines solchen Systems während des ABS-Eingriffs (z.B. Motorrad-ABS-Unfälle in [Hau05]) zu Situationen führen kann, die riskanter sind, als wenn das System überhaupt nicht

verbaut gewesen wäre.
Während bis vor wenigen Jahren der Ausfall eines Fahrzeugrechners im Automobil schlimmstenfalls den Ausfall einer Funktion (z.B. 1967 Injection Control; s. Abbildung 1.1) ohne Gefährdung nach sich zog, wird bei zukünftigen Systemen (z.B. Vehicle Dynamics Controls: ABS (1978), ASR, ESP (1995)) eine fehlerhafte Reaktion auf einen Defekt häufig auch eine Gefährdung für die Fahrzeuginsassen und andere beteiligte Verkehrsteilnehmer darstellen [BJ04].
Hieraus resultieren nachvollziehbarerweise stetig zunehmende Anforderungen an die Sicherheit bzw. Zuverlässigkeit dieser Fahrzeug-Systeme. Um diesen Anforderungen gerecht werden zu können, müssen immer mehr, teilweise vernetzte, Systeme in die Fahrzeuge integriert werden. Die Folge daraus ist, dass deren Systemarchitektur, bei gleichzeitig marktbedingt kürzeren zur Verfügung stehenden Entwicklungszeiten [KCFG04], immer komplexer wird. Der Verlauf des Komplexitätszuwachses von Fahrerassistenzsystemen, hier festgemacht an den *Lines of Code*, über der Zeit ist in Abbildung 1.1 skizziert.

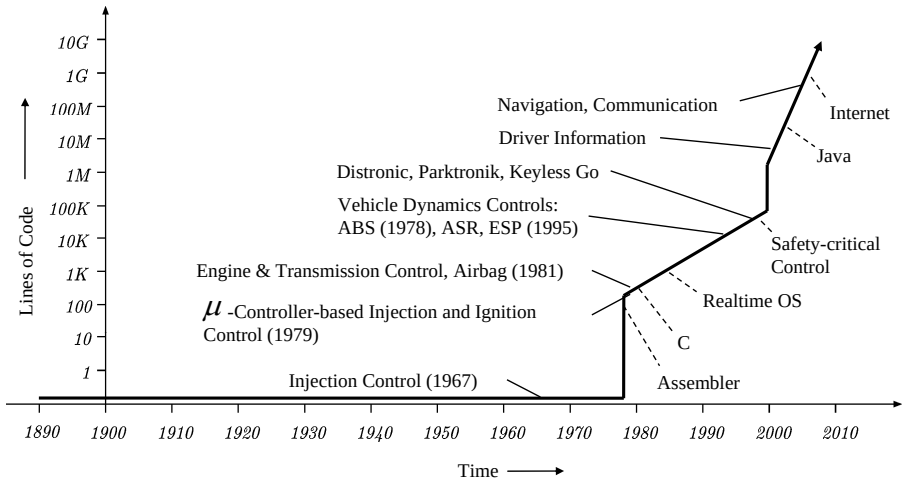


Abbildung 1.1: Komplexität von Fahrzeugsystemen [KCFG04]

Dieser Komplexitätszuwachs führt dazu, dass strukturierte Entwicklungs-Methoden und -Prozesse in Zukunft eine immer größere Rolle spielen werden.
Zusätzlich zeigt die Realität, dass die Verlässlichkeit von komplexen Verkehrssystemen nicht alleine durch Prüfung erreicht werden kann, sondern bereits in der Planung und Projektierung als Bestandteil eines integralen Sicherheitskonzeptes bzw. der Sicherheitsplanung mittels geeigneter Methoden in das System hinein entwickelt wer-

den sollte (siehe nachstehendes Zitat von N. Leveson [Lev01]). Dies nicht zuletzt vor dem Hintergrund, dass ein nachträgliches Hinzufügen von (Sicherheits-)Funktionalität ein System noch komplexer und damit anfälliger für Fehlverhalten macht [TO02].

„Safety must be designed into a System“

In der Literatur (z.B. [BS02, Bas96, Bra04, OS04]) lassen sich drei grundlegende Ansätze der Sicherheitsplanung identifizieren.
Der *empirische* Ansatz basiert auf dem *trial and error*-Prinzip und ist für die Entwicklung von Fahrzeugsystemen absolut unpraktikabel. Hierbei wird das System basierend auf im laufenden Betrieb gewonnenen Erfahrungen der Endverbraucher (weiter)entwickelt. Für die Automobilbranche heißt das, dass Fahrzeugsysteme, bevor die von ihnen ausgehenden Gefährdungen identifziert wurden, am Kunden getestet werden. Der Kunde würde demzufolge vorsätzlich potenziell auftretenden Gefährdungen ausgesetzt, was sowohl aus gesellschaftlichen als auch aus produkthaftungsrechtlichen Gründen nicht vertretbar ist.
Dem empirischen Ansatz gegenüber steht die *maßnahmenorientierte* Sicherheitsplanung. Im Zuge dieses Ansatzes wird von den Systementwicklern die Frage gestellt, welche überhaupt möglichen und denkbaren Sicherheitsmaßnahmen implementiert werden können, um das System so sicher wie möglich zu gestalten. Dieser Ansatz birgt ein erhebliches wirtschaftliches Risiko (vgl. auch Abschnitt 1.3.2), da in eine solche Betrachtung weder die Kosten noch die Wirksamkeit der Maßnahmen mit einfließen.
Einen Kompromiss dieser beiden extremen Ansätze zur Sicherheitsplanung repräsentiert der *risikoorientierte* Ansatz, welcher eine Risikoanalyse voraussetzt und damit die hier vorliegende Arbeit zu Teilen motiviert. Risikoorientierte Ansätze stellen mit der Einbeziehung von Kosten und Wirksamkeit geplanter Maßnahmen in eine probabilistische Sicherheitsbeurteilung die modernsten und für Vergleichszwecke übersichtlichsten Vorgehensweisen dar. Die wesentlichen Vorteile dieser risikoorientierten Ansätze zur Identifizierung von Sicherheitsanforderungen bestehen darin, dass die für die Risikoberechnung erforderlichen Rechengrößen ingenieurmäßig erfassbar sind, und die menschliche Zuverlässigkeit und die technische Verfügbarkeit in ein angemessenes Verhältnis zur technischen Sicherheit gerückt werden. [Bra04, OS04]
Eine frühzeitige Fehlervermeidung ist nicht nur aus Gründen der angestrebten Systemsicherheit unverzichtbar, sondern in besonderem Maße auch unter wirtschaftli-

chen Gesichtspunkten erstrebenswert. Dies vor dem Hintergrund, dass sich die größten Einsparpotentiale dadurch ergeben, dass Fehler in der Wertschöpfungskette so früh wie möglich erkannt und mittels geeigneter Maßnahmen abgestellt werden. Dieser Sachverhalt wird durch die vielzitierte *10er Regel* (s. Abbildung 1.2) beschrieben. Diese Erfahrungsregel aus dem Qualitätsmanagement besagt, dass die Kosten der Fehlervermeidung bzw. der Fehlerbehebung von Wertschöpfungsgrenze zu Wertschöpfungsgrenze um den Faktor 10 steigen. So sind beispielsweise die entstehenden Kosten zur Fehlervermeidung zehnmal höher, wenn Fehler in der Entwicklungsphase gemacht, aber erst in der Arbeitsvorbereitung entdeckt werden [Haf05].

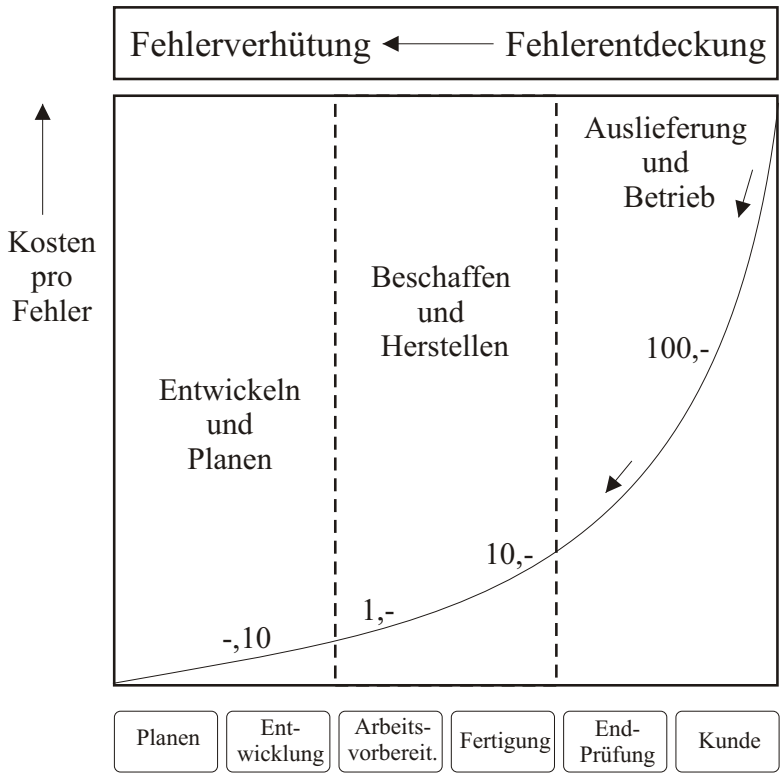


Abbildung 1.2: Zusammenhang der Fehlerverursachung und der Fehlerkosten in verschiedenen Produktlebensphasen (in Anlehnung an [Haf05])

Eben aus den genannten Gründen und basierend auf sich verändernden gesetzlichen und produkthaftungsrechtlichen Rahmenbedingungen, welche wesentlich höhere Anforderungen an eine Fahrzeug-Systementwicklung stellen, als sie beispielsweise in gesetzlichen Regelungen (z.B. ECE-RL) verankert sind, ist es nachvollziehbar,

dass die Nachfrage nach normativen Vorgaben hinsichtlich strukturierter und praktisch anwendbarer Risikoanalyse-Ansätze in der Automobilbranche immer weiter wächst.
Abschnitt 2.1 gibt einen Überblick über die derzeit anwendbaren Normen im Bereich der Entwicklung sicherheitskritischer E/E/PE-Fahrzeugsysteme und deren Eingliederung in die gültige Rechtsordnung.

1.3 Ausgangssituation und Problemstellung

In Abschnitt 1.1 ist das Ziel der vorliegenen Arbeit formuliert, der oftmals unbegründeten Überdimensionierung von Sicherheitsfunktionen strukturiert entgegenzuwirken.
Die Auslegung von Sicherheitsfunktionen, aber auch die Anforderungen an den Entwicklungsprozess dieser Funktionen, basieren heutzutage meist auf den Ergebnissen von Ansätzen, welche unter dem Begriff *Risikoanalyse* subsummiert werden. Es wird deutlich, dass es keine einheitliche Vorgehensweise zur Identifikation und Bewertung von Gefährdungen gibt. Vielmehr existiert eine große Anzahl von nebeneinander angewendeten Ansätzen, welche sich unterschiedlicher Techniken bedienen.
Diese Methoden-Vielfalt wird in Abschnitt 1.3.1 allgemein diskutiert, bevor in Abschnitt 1.3.2 die in der Automobil-Branche vorwiegend methodengebenden Normen zur funktionalen Sicherheit eingeführt und das in Abschnitt 1.1 dargestellte Ziel motiviert wird.

1.3.1 Vorherrschende Methodenvielfalt

Die Durchführung einer Risiko- und Gefährdungsanalyse ist als wesentlicher Bestandteil der Entwicklung von sicherheitsrelevanten Systemen unumgänglich. Dies hat sowohl gesellschaftliche (vgl. Abschnitt 1.2) als auch normative Gründe (vgl. Abschnitt 2.1).
Um der Anforderung der normkonformen Durchführung einer Risikoanalyse Folge zu leisten, werden dem Entwickler heutzutage eine Vielzahl von Analyseansätzen, welche ihre Wurzeln in den unterschiedlichsten Branchen haben, an die Hand gegeben. Diese Verfahrensvielfalt, welche häufig auf einen sehr flexiblen normativen Rahmen mit großen interpretatorischen Freiheiten zurückzuführen ist, wird in der Literatur kontrovers diskutiert.

Braband [Bra05] steht der Verfahrensvielfalt, wie sie dem Entwickler von Eisenbahnautomatisierungssystemen in der DIN EN 50129 [EN50129] bereitgestellt wird eher kritisch gegenüber. Zwar konnte die in [EN50129] vorgeschlagene Vorgehensweise zur Risikoanalyse bisher auf fast alle aufgetretenen Anwendungsfälle, dies keinesfalls nur auf die Eisenbahnsicherungstechnik beschränkt, erfolgreich angepasst werden, und so lösungsunabhängige, diskriminierungsfreie Sicherheitsanforderungen liefern, allerdings konnte sich aufgrund der uneindeutigen Formulierung noch keine Vorgehensweise als Standard etablieren. Die Ergebnisse der auf dieser Norm basierenden Risikoanalysen sind vielmehr allesamt Unikate mit nur geringem Überdeckungsgrad und daher verhältnismäßig schlecht vergleichbar.
N. Leveson vertritt in [Lev01] hinsichtlich einer angestrebten Vereinheitlichung von Vorgehensweisen, welche in einer Standard-Vorgehensweise mündet, eine andere Meinung. N. Leveson sieht in einer immer weiter fortschreitenden Vereinheitlichung die Gefahr, dass sich Entwickler von sicherheitskritischen Systemen dazu verleiten lassen einem *Kochrezept* zu folgen, ohne es kritisch zu hinterfragen:

> „By following cookbook solutions, we are very likely to find that we feel satisfied and our jobs are greatly simplified, but risk ist not appreciably reduced.“ [Preface, [Lev01]]

Unabhängig davon, ob eine Standard-Vorgehensweise bzw. Standard-Methode erstrebenswert ist oder nicht, sind sich die Autoren von [Bra05] und [Lev01] einig, dass letztendlich alle zur Durchführung von Risikobetrachtungen zur Verfügung stehenden *Beschreibungsmittel und Methoden*, im Folgenden häufig unter *Technik(en)*[3] zusammengefasst, ihre Vor- und Nachteile haben. Welche dies im einzelnen sind, wird in Kapitel 3 detailliert beschrieben.
Schon hier soll jedoch hervorgehoben werden, dass die meisten der in den Normen genannten Methoden auf einer mehr oder weniger informellen Beschreibung von kausalen Wirkungsketten basieren, welche sehr anfällig für Analysefehler [Slo06] sind. Bei kontinuierlich steigender Komplexität (vgl. Abschnitt 1.2) von modernen Fahrzeugen bzw. Fahrerassistenzsystemen, an deren Entwicklung eine Vielzahl von Personen mit unterschiedlichsten Kenntnisständen aus verschiedenen Bereichen beteiligt sind

[3] Als Technik wird hier nicht die (Formale) Technik verstanden, welche nach [ES99] als das Verwenden eines (formalen) Beschreibungsmittels unter Anwendung einer bestimmten Methode definiert ist, sondern die Technik als Konglomerat von Beschreibungsmitteln und Methoden im Sinne (EN 50128).

und die Interaktionen zwischen vernetzten Hardware- und Softwarekomponenten, aber auch die Mensch-Maschine-Interaktion, zumeist schwer zu überblicken sind, ist ein informelles Vorgehen zur Risikoanalyse quasi von vorne herein zum Scheitern verurteilt.
Einen großen Vorteil haben diesbezüglich nach [Sch03, SCEH03] formale Techniken, welche es erlauben auch zeitabhängige Ursache-Wirkungsbeziehungen in ihrem Verhalten mathematisch eindeutig, präzise und nachvollziehbar [Sch99b] zu beschreiben. Des Weiteren bietet eine formalmodellbasierte Repräsentation von methodischen Grundkonzepten die Möglichkeit, die Methode formal prüfbar und konsistent zu entwickeln und anzuwenden. Bis dato sind diese in der Informatik weit verbreiteten formalen Beschreibungsmittel in der Ingenieurspraxis noch wenig verbreitet [Slo06].

1.3.2 Problem(dar)stellung

In Abschnitt 1.3.1 ist die Problematik der vorherrschenden Vielfalt von Methoden zur Durchführung von Risikoanalysen für sicherheitsrelevante Systeme aufgezeigt.
Dieser Tendenz entgegenwirkend wird für den Automobilbereich seit einigen Jahren eine Methode zur Gefährdungsidentifikation und Risikobewertung diskutiert, wie sie im Automotive-Derivat der Sicherheitsgrundnorm IEC 61508, dem ISO 26262 (s. Abschnitt 2.1.2), dargestellt ist. Auch wenn sich diese qualitative Methode, welche schon heute in vielen Bereichen bei OEMs und Zulieferern Anwendung findet – dies ohne den aktuell geltenden gesetzlichen Anforderungen zu genügen – voraussichtlich in Zukunft im Automobilbereich durchsetzen wird, ist diese nicht frei von Kritik.
So lastet Paulus in [Pau07] dem Verfahren an, dass verschiedene ungeübte Anwender bei der Analyse ein und desselben Systems aufgrund von Interpretationsschwierigkeiten zum Teil sehr unterschiedliche Ergebnisse erzielen. Dies ist vor allem darauf zurückzuführen, dass die zur Ableitung der Sicherheitanforderungen erforderlichen Parameter – ähnlich wie bei verschiedenen anderen Methoden (z.B. der SIL Bestimmung nach IEC 61508) – stark von der sehr subjektiven Meinung von Anwendern abhängig ist.
Folgende Beispiele für Expertenschätzungen zeigen exemplarisch (aber deutlich) auf, dass die Problematik der Ergebnisabhängigkeit von personengebundenen Eingangswerten keineswegs branchenspezifisch und daher auch im Bereich der Elektronikentwicklung im Automobilbau nicht zu vernachlässigen ist.
So werden in [Mal08] die Nebenwirkungen des exponenziellen Anstiegs der Bio-

kraftstoffproduktion von verschiedenen Experten analysiert. Es werden kontroverse Diskussionen dargelegt, ob und in welchem Maße die Biokraftstoffe für hohe Lebensmittelpreise mitverantwortlich sind. Die Expertenschätzungen schwanken hier zwischen 3 und 75 Prozent.
Ein weiteres Beispiel dafür, in welchem Maße Expertenschätzungen divergieren können wird in [HL98] beschrieben. Bei der Schätzung der Anzahl sog. „irregulärer" Zuwanderer in Deutschland liegen die Experten um eine Zehnerpotenz auseinander (100.000 vs. 1.000.000 Menschen).
In [Fro06] dagegen wird ein eher techniklastiges Schätzproblem beschrieben. Hierbei geht es um die Abschätzung von Software-Entwicklungs-Aufwänden. Im Rahmen der dort beschriebenen Untersuchung wurden Software-Projekte auf Basis einer Grobspezifikation durch Experten individuell geschätzt. Nach Abschluss der Projekte wurde eine Nachkalkulation durchgeführt, welche zu Tage brachte, dass Projektvorhaben im Mittel um 40 Prozent unterschätzt wurden.
Die Intention dieser Auflistung ist es keineswegs grundsätzlich gegen Expertenschätzungen zu argumentieren. In vielen Bereichen würde man ohne solche Expertenschätzungen – ein Experte hat sich schließlich nach [HS08] 10.000 h mit seinem Fachgebiet auseinandergesetzt – mit großer Wahrscheinlichkeit zu noch weniger belastbaren Aussagen kommen als mit diesen „optimierungsbedürftigen" Schätzungen. Der Leser soll lediglich hinsichtlich der Aussagekraft solcher Ergebnisse sensibilisiert werden.
Des Weiteren soll an dieser Stelle darauf hingewiesen werden, dass auf Expertenschätzungen basierende qualitative Methoden zur Risikoabschätzung häufig sehr konservative Ergebnisse, und damit unnötig hohe Sicherheitsanforderungen, liefern [Bep08].
Hierdurch wird zwar in den meisten Fällen das festgelegete Risikoakzeptanzkriterium erfüllt, dies aber häufig auf Kosten einer, den subjektiven Abschätzungen zugrunde liegenden Überdimensionierung (s. Abb. 1.3) der Sicherheitsfunktionen, wodurch nicht zu vernachlässigende Mehrkosten entstehen.
So ist wie in [DIN FB 144] beschrieben grundsätzlich anzustreben, dass das Restrisiko das akzeptierte Risiko möglichst weit unterschreitet. Dies ist jedoch nicht nur eine Frage der technischen Machbarkeit, sondern vielmehr eine wirtschaftliche Optimierungsfrage. Maßgebend sind hier die Grenzkosten der Risikominderung, also die Mehrkosten je Einheit der Risikominderung verglichen mit der Bereitwilligkeit des

Marktes, Sicherheit zu honorieren.
Auch vor dem Hintergrund eines vom DVR verabschiedeten Beschlusses [DVR06] sind solche Mehrkosten gerade bei der Entwicklung von zukünftigen Fahrerassistenzsystemen zu vermeiden. Dieser Beschluss fordert, neben der einfachen Anwendbarkeit des Systems, sowohl einen plausiblen und praktischen Nutzen für den Verkehrsteilnehmer als auch ein angemessenes Preis-Leistungs-Verhältnis.

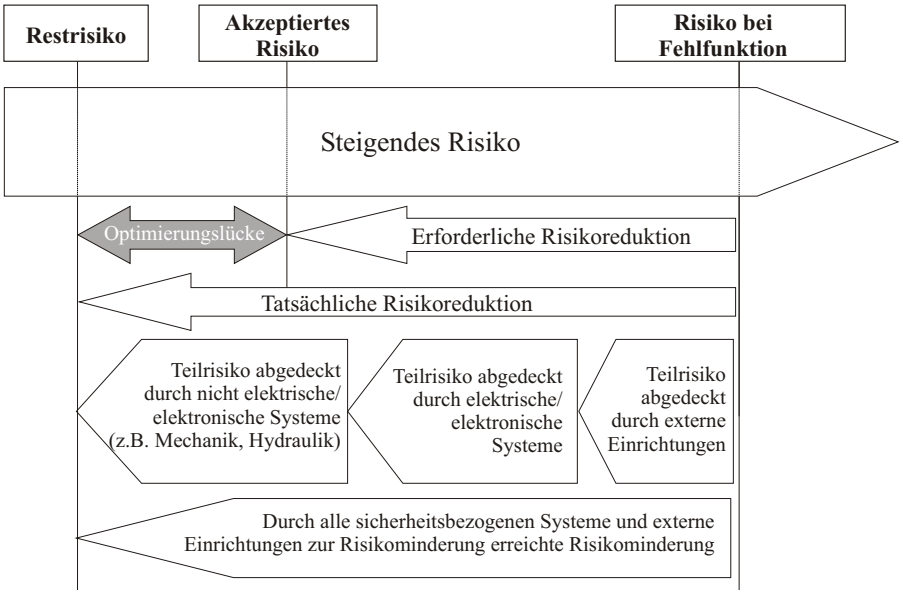


Abbildung 1.3: Optimierungslücke (in Anlehnung an [Rau08])

Aufgrund der zuvor dargelegten Problematik bei der Anwendung von qualitativen Verfahren erscheinen quantitative Methoden besser zur Risikobeurteilung geeignet zu sein. Bei genauerer Betrachtung von quantitativen Risikobeurteilungen wird jedoch deutlich, dass mit der Anzahl der zu modellierenden Parameter nicht nur der Modellierungsaufwand steigt, sondern in der Regel die Aussagegenauigkeit der Ergebnisse sinkt, da die für die quantitative Analyse erforderliche Datenbasis in den meisten Fällen nicht oder nur unter Aufwendung sehr großer Ressourcen in ausreichendem Umfang zur Verfügung steht.
Diese Problematik ist vor allem im Bereich der Softwareentwicklung nachvollziehbar, da diese hauptsächlich durch organisatorische Rahmenbedingungen (z.B. Verfügbarkeit von Personal etc.) geprägt wird, deren Einfluss sehr schwierig zu quantifizieren ist. In solchen Fällen ist grundsätzlich von der Durchführung quantitativer Analysen abzusehen, da falsche, fehlende oder unvollständige Daten stets zu Ergebnissen

führen, welche die Aussagekraft derselben erheblich verfälschen [HMMR96].
Quantitative Methoden können demnach nur dann sinnvoll eingesetzt werden, wenn Eintrittswahrscheinlichkeit und Schadensausmaß von kritischen Ereignissen in präzisen Werten und eindeutigen Dimensionen angegeben oder berechnet werden können.
Aufgrund der zuvor dargestellten Vor- und Nachteile qualitativer und quantitativer Methoden besteht der Bedarf an einem optimierten Verfahren, welches die Benutzerfreundlichkeit von qualitativen Methoden mit der ingenieursmäßig nachvollziehbaren Modellierung von quantitativen Methoden vereint [Bep08].
Im Zuge dieser Bestrebung werden in verschiedenen Branchen immer stärker sogenannte semi-quantitative Methoden eingesetzt. Diese haben den Vorteil, dass mit ihnen empirische Ereignisdaten ebenso wie Expertenwissen berücksichtigt und damit subjektive Einschätzungen und objektive Erfahrungen miteinander verknüpft werden können.
In diesem Sachverhalt begründet liegt die Motivation des in Abschnitt 1.1 beschriebenen Zieles dieser Arbeit, das qualitative Vorgehen zur ASIL-Bestimmung nach ISO 26262 mit Hilfe von quantitativen Methodenmerkmalen zu objektivieren.

1.4 Struktur der Arbeit

Die Arbeit ist in zehn Kapitel gegliedert, welche sukzessiv ihre Beiträge zum Verständnis der entwickelten EmMORI-Methode liefern und in der Beschreibung eines Anwendungsbeispiels münden. Abbildung 1.4 stellt die wesentlichen Zusammenhänge der einzelnen Kapitel dar.
Nachdem in Kapitel 1 die modellbasierte Objektiverung von, durch subjektive Einflüsse bzw. Einstellungen geprägte, Expertenschätzungen motiviert wurde, setzt sich Kapitel 2 im Detail mit den rechtlichen Rahmenbedingungen im Umfeld der Entwicklung von E/E/PE-Systemen in Personenkraftwagen auseinander.
In Kapitel 3 werden strukturiert potenziell zur Lösung des Objektivierungsproblems anwendbare Techniken der Sicherheits- und Zuverlässigkeitsanalyse vorgestellt und hinsichtlich ihrer Stärken und Schwächen analysiert.
Im darauf folgenden Kapitel 4 werden zunächst die verschiedenen an die EmMORI-Technik gestellten Anforderungen identifziert. Diese Anforderungen verkörpern anschließend die Bewertungskriterien eines die verschiedenen Techniken gegenüberstellenden paarweisen Vergleiches.

Zur Entwicklung einer Methode zur Objektivierung der Risikoanalyse nach ISO 26262 bedarf es eines hinreichenden Verständnisses des zu objektivierenden Gegenstandes (hier: Automotive Safety Integrity Level (ASIL)). Daher wird der ASIL in Abschnitt 5 zunächst einmal in seinem fachspezifischen automobilen Kontext eingeführt, definiert und eingebettet, bevor in Kapitel 6 seine terminologische Einordnung in ein Begriffsgebäude zur funktionalen Sicherheit im Automobilwesen diskutiert wird.
Kapitel 7 beschreibt die Anwendung der verschiedenen nach ISO 26262 und IEC 61508 den Stand der Technik abbildenden und daher im Automobilsektor gebräuchlichen Risikoanalyse-Ansätze auf eine Beispielfunktion (Abblendlicht).
In Kapitel 8 wird die sich hinter dem EmMORI-Konzept verbergende Methode (Modellbildungs-, Simulations- und Analyse-Ansatz) erläutert und validiert, bevor sie in Kapitel 9 auf die bereits in Kapitel 7 eingeführte Funktion „Abblendlicht“ angewendet wird.
Kapitel 10 schließt die Arbeit mit einer Zusammenfassung der wesentlichen gewonnenen Erkenntnisse der Analysen und einem Ausblick hinsichtlich potenzieller zukünftiger wissenschaftlicher Herausforderungen.

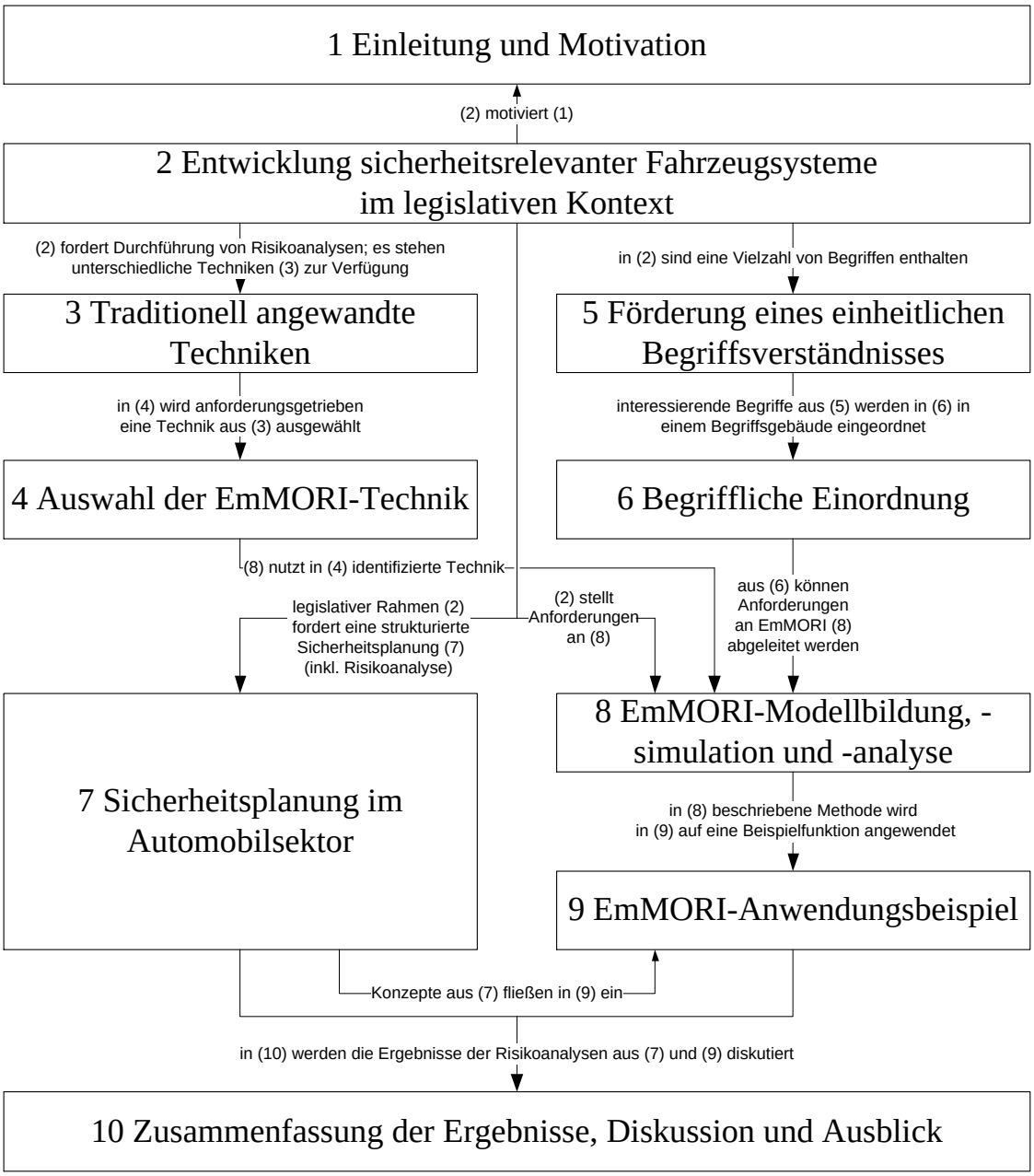


Abbildung 1.4: Gliederung der Arbeit

Kapitel 2

Entwicklung sicherheitsrelevanter Fahrzeugsteuerungssysteme im legislativen Kontext

Die Entwicklung von zukünftigen elektrischen/elektronischen/programmierbaren elektronischen (E/E/PE) Fahrzeugsystemen befindet sich, wie in Kapitel 1 angedeutet, in einem von der vorherrschenden Marktsituation, einem stetigen Komplexitätszuwachs und den sich verändernden legislativen Rahmenbedingungen bestimmten Spannungsfeld. Auf eben diese legislativen Randbedingungen wird in den nachfolgenden Abschnitten im Detail eingegangen.

2.1 Legislativer Hintergrund

Häufig wird die Rechtsordnung als hierarchische Struktur in Form einer Pyramide („Pyramide des Rechts“) dargestellt. Dieser pyramidenartige Aufbau (s. Abbildung 2.1), auf welchen in Abschnitt 2.1.1 im Detail eingegangen wird, basiert auf der langen Tradition, in der die verschiedenen Rechtsquellen stehen. In einer modernen Gesellschaft besitzen nicht alle Rechtsquellen denselben Rang, vielmehr haben einige Vorrang vor anderen. Diese Rangordnung besagt ganz allgemein, dass:

- EG/EU-Recht bricht Bundesrecht
- Bundesrecht bricht Landesrecht
- spezielle Norm geht der allgemeineren Norm vor

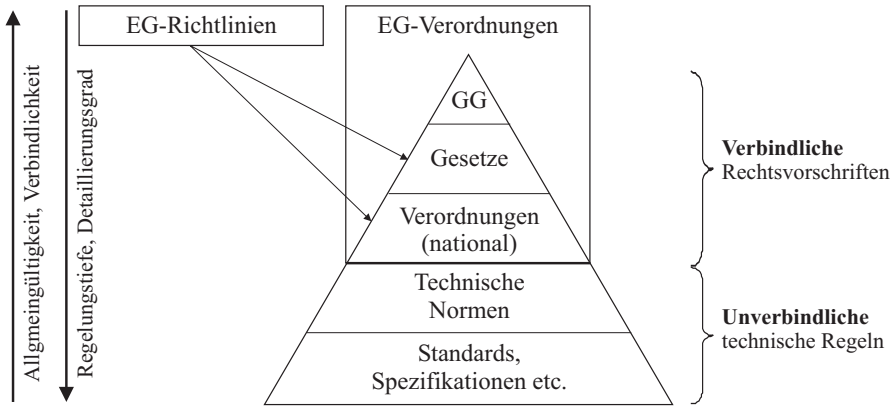


Abbildung 2.1: Pyramide des Rechts [Los07]

- jüngere Norm geht der älteren Norm vor

Wichtig ist demnach, dass jedes Gesetz bzw. jede Norm mit allen übergeordneten Gesetzen vereinbar ist.
In einer komplexen Gesellschaft wie der heutigen Industriegesellschaft hat das Recht eine Reihe von Regeln entwickelt, um örtliche und zeitliche Normenkonflikte zu vermeiden. Hierbei handelt es sich um empirische Regeln, die der praktischen Handhabung des Rechts dienen. Sie entstehen unter dem Druck momentaner Notwendigkeiten und sind deshalb nicht unbedingt aufeinander abgestimmt [Los07].
Die wesentlichen für die Entwicklung von FAS relevanten Gesetze, Normen und Richtlinien lassen sich wie in Abschnitt 2.1.1 beschrieben in das geltende Rechtssystem eingliedern.

2.1.1 Europäische und nationale verbindliche Rechtsvorschriften

An oberster Stelle des in Deutschland geltenden Rechtes steht das Grundgesetz (GG) [GG49]. Dieser sehr allgemein gehaltene Gesetzestext hat zunächst scheinbar noch keinen direkten Bezug zur Entwicklung von FAS. Dieser Bezug wird jedoch bei detaillierterer Betrachtung bereits in Artikel 2 Abs. 2, welcher für jeden Bürger das Recht auf körperliche Unversehrtheit fordert, deutlich. Pflichten und Rechte welche sich für die Hersteller von sicherheitsrelevanten technischen Einrichtungen ergeben, werden in verschiedenen dem GG untergeordneten Gesetzen verfeinert. Zur spezifischen Anwendung dieser Gesetze werden Verordnungen formuliert. Diese Gesetze

und Verordnungen müssen gemäß der in Abschnitt 2.1 erläuterten Rangordnung europäische Richtlinien in nationales Recht umsetzen.
EG-Verordnungen werden innerhalb der Mitgliedsstaaten nicht in nationale Gesetze überführt, da diese mit ihrer Verabschiedung unmittelbar gültig und damit verpflichtend sind.
Das GG, die Gesetze und Verordnungen können unter dem Terminus der „verbindlichen Rechtsvorschriften“ (s. Abb. 2.1) zusammengefasst werden.
Der untere Teil der Pyramide visualisiert die Ebene der „unverbindlichen technischen Regeln“ deren Inhalte, wie es der Name sagt, zwar nicht verbindlich sind, welche aber z.B. von Gerichten in Straf- und (Produkt-)Haftpflichtfällen herangezogen werden, um die anerkannten Regeln der Technik („Stand der Technik“) zu ermitteln [SIA08]. Hierbei handelt es sich sowohl um Technische Normen, welche durch ein offizielles Gremium erarbeit und der Öffentlichkeit zur Verfügung gestellt werden, als auch um Standards und Spezifikationen, für deren Generierung sich ein Konsortium zusammenfindet, welches den entstandenden Standard zahlenden Mitgliedern zur Verfügung stellt [Hän08].
Wie bereits zuvor beschrieben ist im Grundgesetz das Recht auf körperliche Unversehrtheit verankert. Die Europäische Union (EU) fordert mit der Produktsicherheitsrichtlinie, dass der Mensch vor den Gefahren eines Gerätes oder Produktes geschützt werden muss. Dort heißt es, dass alle Produkte, die in Verkehr gebracht werden, sicher sein müssen. Unter dem Produkt versteht diese Richtlinie jedes System bzw. Gerät, welches für Verbraucher bestimmt ist bzw. unter vernünftigerweise vorhersehbaren Bedingungen von Verbrauchern genutzt werden könnte. Ein Gerät gilt als sicher, wenn es bei normaler oder vernünftigerweise vorhersehbarer Verwendung keine oder nur geringe Gefahren für den Menschen birgt [2001/95/EG]. Diese Richtlinie wurde mit dem Geräte- und Produktsicherheitsgesetz in nationales Recht umgesetzt, indem 14 Verordnungen zum Geräte- und Produktsicherheitsgesetz erlassen wurden, welche sich mit Spielzeugen, Gasverbrauchseinrichtungen oder Maschinen (z.B. Fahrzeuge zur Personenbeförderung) befassen.
Parallel zum Geräte- und Produktsicherheitsgesetz, ist vom Hersteller eines FAS gleichermaßen den Anforderungen der Straßenverkehrs-Zulassungs-Ordnung (StVZO) [StVZO09] Folge zu leisten. So fordert §30. Abs. 1 StVZO, dass Fahrzeuge so gebaut und ausgerüstet werden, dass ihr verkehrsüblicher Betrieb niemanden schädigt oder mehr als unvermeidbar bzw. normal gefährdet, behindert oder belästigt.

Auf der Ebene der Verordnungen weist §2 Abs. 4 der Fahrzeug-Zulassungsverordnung (FZV) darauf hin, dass der zur Prüfung vorgestellte Typ eines Fahrzeuges, eines Systems (z.B. FAS), eines Bauteils oder einer selbständigen technischen Einheit die einschlägigen Vorschriften und technischen Anforderungen erfüllen muss. Durch diese Forderung werden die im Folgenden dargestellten, den Stand der Technik beschreibenden Normen und Standards aufgewertet, und §2 Abs. 4 der Fahrzeug-Zulassungsverordnung (FZV) [FZV06] gilt nur noch subsidiär.
Auf der Ebene der Technischen Normen muss insbesondere die ISO 26262 als für die Entwicklung von zukünftigen E/E/PE-Fahrzeugsystemen relevante Norm genannt werden, auf welche im Abschnitt 2.1.2 im Detail eingegangen wird.
Zudem ist die Sicherheitsgrundnorm IEC 61508 (s. Abschnitt 2.1.2), welche die Basis der ISO 26262 darstellt, zu beachten. Auf der unverbindlichsten Ebene der Standards und Spezifikationen ist beispielsweise die Entwicklungspartnerschaft mehrerer Automobilhersteller und -zulieferer AUTOSAR zu nennen, deren Ziel einheitliche Standards im Bereich Software- und Hardwareentwicklung sind, um Fehler zur minimieren. Ebenso sind hier die Bestrebungen des RESPONSE3-Konsortiums einzuordnen, deren Code of Practice als Richtlinie für die Entwicklung und Validierung von sicheren FAS dienen soll [Kis08].

2.1.2 Die Sicherheitsgrundnorm IEC 61508 und ihr Automotive-Derivat ISO 26262 als unverbindliche technische Regeln

Im Zuge der Entwicklung von sicherheitsrelevanten Systemen werden dem Hersteller verschiedene Normen an die Hand gegeben, deren Anwendung die Erfüllung der in den übergeordneten Gesetzen und Verordnungen gestellten Anforderungen erleichtern soll. Bei der Entwicklung von fahrzeugtechnischen E/E/PE-Systemen kann der Hersteller heute zwei unterschiedliche Wege beschreiten.
Zum einen kann er seine Entwicklungsprozesse an der generischen Sicherheitsgrundnorm IEC 61508 orientieren, welche rein rechtlich den aktuellen Stand der Technik zur „Funktionalen Sicherheit“ von E/E/PES definiert. Entscheidet sich der Hersteller für die Anwendung der IEC 61508, kann er jederzeit den notwendigen Beweis liefern, allen Erfordernissen bei der Herstellung sicherheitsrelevanter elektronischer bzw. mechatronischer Einrichtungen entsprochen zu haben.
Eine Vielzahl von Automobilherstellern und -zulieferern stützt ihre Entwicklungsak-

tivitäten schon heute auf der branchenspezifischen Adaption der IEC 61508, der ISO 26262 (s. Abschnitt 2.1.2), obwohl hierfür aufgrund der fehlenden Finalisierung der Norm rechtlich noch keine Basis geschaffen ist. Befürworter der Anwendung der ISO 26262 argumentieren zumeist damit, dass die ISO 26262 bereits weitestgehend abgestimmt ist, weswegen zu erwarten ist, dass ihre Publikation in 2011 erfolgt [Kri09]. Laufende Entwicklungen werden zudem zum Teil erst nach der Veröffentlichung der ISO 26262 in Serie gehen, so dass mit der Anwendung des branchenspezifischen Derivats der IEC 61508 gewissermaßen in Vorleistung gegangen wird, um dem zukünftigen Stand der Technik zu genügen.

IEC 61508

Die wichtigste und am besten etablierte Norm in der umfassenden sicherheitsbezogenen Normenlandschaft (s. Abb. 2.2) ist, wenn auch nicht frei von Kritik, nach wie vor die IEC 61508, welche als ein vorerst letzter Schritt in einer langen Kette von Normen zur funktionalen Sicherheit, die mit den Risikodefinitionen in DIN 31000 und DIN V 19250 begann und mit den DIN V VDE 0801 in Deutschland eine solide Grundlage fand, zu sehen ist. Die Weiterentwicklung der Norm, mit historischem Hintergrund in der Anlagen- und Verfahrenstechnik, ist jedoch auch heute noch nicht abgeschlossen. Derzeit wird die erste Ausgabe überarbeitet; seit dem Jahr 2009 ist ein Final Draft International Standard (FDIS) verfügbar.
Die IEC 61508 beschreibt einen Katalog von etwa 600 Anforderungen, welche an die Entwicklung sicherheitsbezogener E/E/PE-Systeme unter Gesichtspunkten der funktionalen Sicherheit gestellt werden. Die Anwendung der IEC 61508 unterscheidet sich von der bisher oft in der Sicherheitstechnik verwendeten Vorgehensweise, da diese Norm nicht nur einen Teil des Systems in einer Entwicklungsphase, sondern das ganze System innerhalb seines gesamten Lebenszyklus betrachtet.
Sie schildert einen allgemeinen anforderungsorientierten Lösungsweg von den ersten Entwicklungsschritten über den Einbau bis hin zur Außerbetriebnahme für die Gesamtheit der Tätigkeiten während des Sicherheitslebenszyklus für E/E/PE-Systeme, welche Sicherheitsfunktionen zu realisieren haben. Dieser allgemeine Lösungsweg wurde gewählt, um ein branchenunabhängiges, sinnvolles und konsistentes technisches Verfahren für alle elektrischen Sicherheitssysteme bereitzustellen. IEC 61508 kann sowohl direkt von Industrieunternehmen verwendet als auch zur Ableitung

branchenspezifischer Normen eingesetzt werden, was als eines der Hauptziele der Norm hervorgehoben wird.

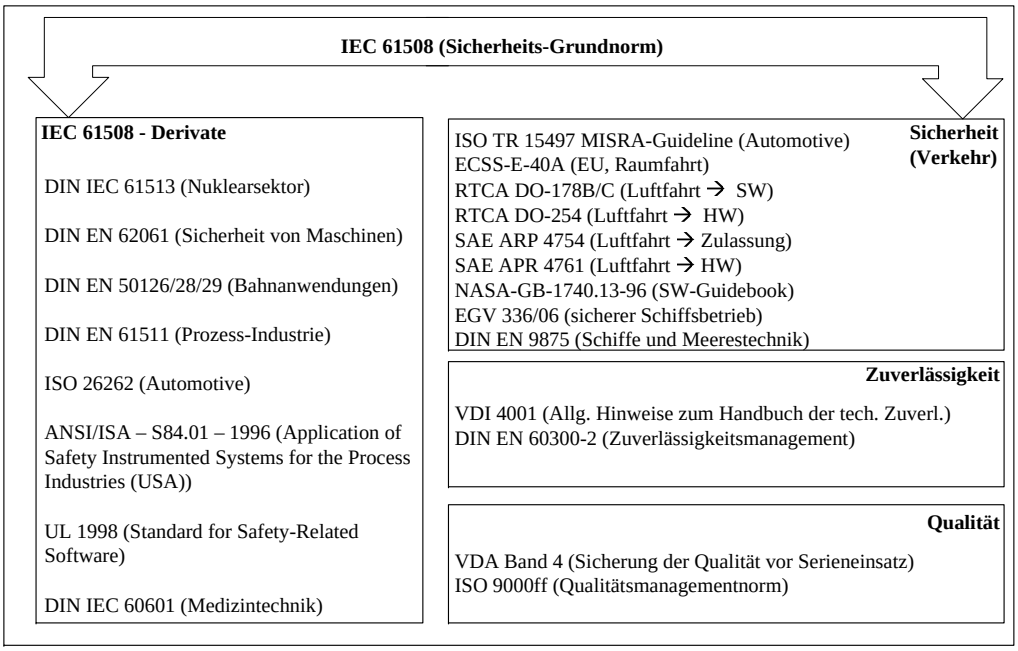


Abbildung 2.2: Normenlandschaft [SBS08]

Einige solcher abgeleiteten Branchennormen, wie z.B. IEC 61511 für die Prozessindustrie, IEC 61513 für den Nuklearsektor oder IEC 62061 für die Maschinenindustrie, seien hier nur kurz erwähnt, auf den ISO 26262 für die Automobilbranche wird später detaillierter eingegangen.
Ist eine solche abgeleitete branchenspezifische Norm verabschiedet, tritt nach Ablauf eines Übergangszeitraumes die IEC 61508 in den Hintergrund und die Anforderungen des Branchen-Derivates bekommen bindenden Charakter (vgl. auch Abschnitt 2.1). Dies gilt auch für den Fall, dass das branchenspezifische Derivat geringere Anforderungen an das System bzw. den Entwicklungsprozess des Systems stellt, als es die Sicherheitsgrundnorm getan hat.
Die IEC 61508 selbst setzt sich aus sieben Teilen zusammen, von denen die Teile eins bis vier normativen und die übrigen Teile informativen Charakter haben.
Während Teil 1 das Hauptaugenmerk auf die sehr frühen Phasen des Lebenszyklus (s. Abb. 2.3), also Konzept, Definition des Anwendungsbereiches, Gefährdungs- und Risikoanalyse und Zuordnung von Sicherheitsanforderungen, legt, geht Teil 2 detail-

lierter auf die Realisierungsphase sicherheitsbezogener E/E/PE-Systeme ein.
Der dritte Teil der Norm beschreibt die Anforderungen, welche im Rahmen der Realisierungsphase sicherheitsbezogener Software zu erfüllen sind. Für komplexe Systeme mit integrierter Software ist die Erfüllung der in Teil 3 dokumentierten Anforderungen also unverzichtbar, wenn in Übereinstimmung mit IEC 61508 entwickelt werden soll.

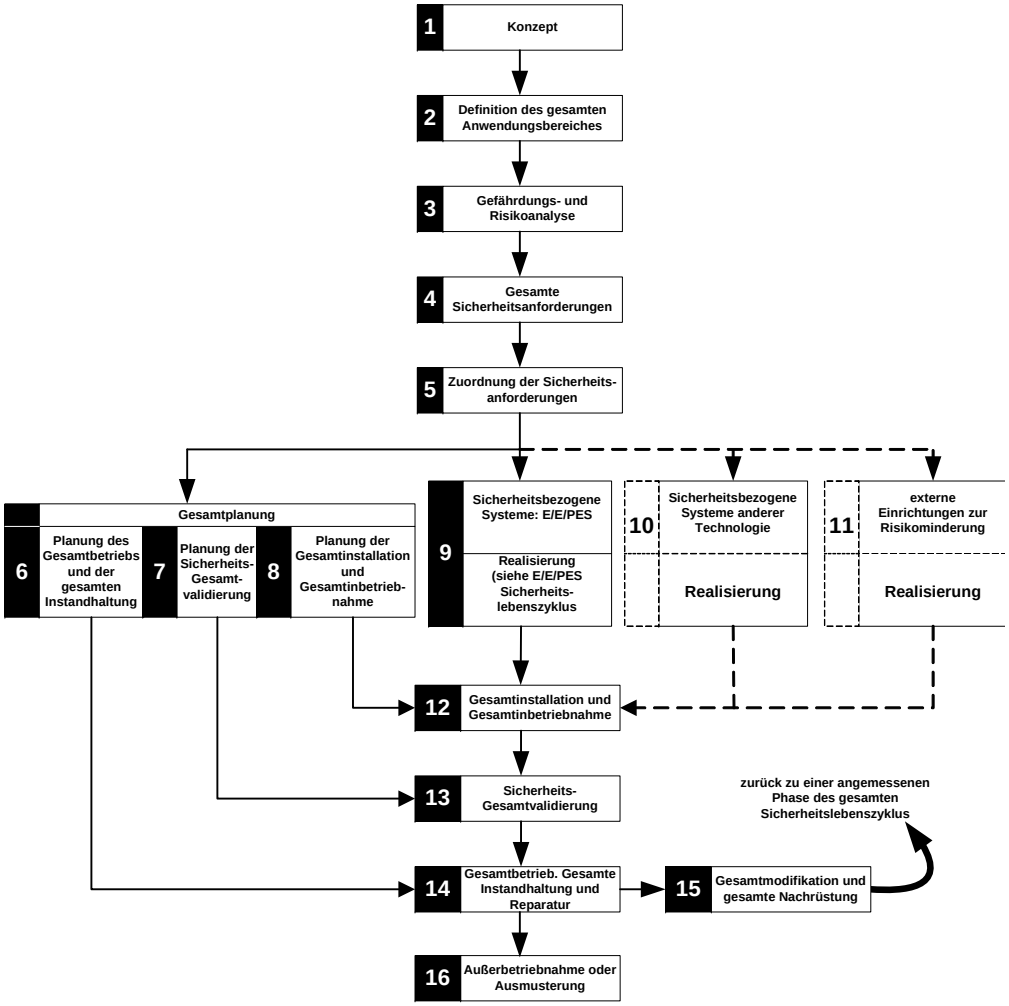
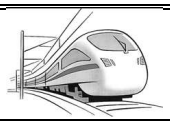


Abbildung 2.3: Sicherheitslebenszyklus nach IEC 61508

Erst der vierte Teil der Norm beinhaltet die Defintionen und Benennungen, die in der gesamten Norm verwendet werden.
Teil 5 als erster informativer Teil dieser Normenreihe – auf diesen Teil wurde zuvor bereits verwiesen – geht im Detail auf den Zusammenhang zwischen Risiko

und Sicherheitsintegrität, sowie verschiedene Methoden, die es ermöglichen einen Sicherheits-Integritätslevel (SIL) für sicherheitsbezogene E/E/PE-System festzulegen, ein. In den ebenfalls informativen Teilen 6 und 7 werden Informationen und Anwendungsrichtlinien und ein Überblick über die verschiedenen Sicherheitsverfahren und -maßnahmen zur Anwendung der Teile 2 und 3 gegeben.
Zur Gewährleistung der oben beschriebenen Anforderungen an die Systemeigenschaften Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit decken die in der IEC 61508 beschriebenen Inhalte den gesamten Lebenszyklus eines sicherheitskritischen Systems ab.
Soll ein höchst zuverlässiges, hochverfügbares und sicheres System entwickelt werden, so bedarf es nach IEC 61508 einer maximalen Übereinstimmung mit den in der Norm geforderten Aktivitäten und Dokumentationen. Um Übereinstimmung mit dieser Norm zu erreichen, muss dargelegt werden, dass diese Anforderungen entsprechend den erforderlichen festgelegten Kriterien erfüllt werden und die Ziele jedes Norm-Abschnitts oder Unterabschnitts erreicht worden sind. Bereits diese Forderung nach strikter Abschnittserfüllung lässt vermuten, dass diese Norm bei Herstellern und Zulieferern aufgrund fehlender branchenspezifischer Sinnhaftigkeit nur teilweise auf Gegenliebe stößt.
Allerdings relativiert die Norm ihre selbst auferlegte Anforderung nach Normerfüllung in Absatz 4.2 (Teil 1) in sich selbst. Es heißt, dass in solchen Fällen, in denen keine internationale anwendungsspezifische Norm vorhanden ist und die IEC 61508 direkt angewendet werden soll, bestimmte festgelegte Anforderungen unnötig sind, und eine begründete Teil-Befreiung (z.B. durch einen amtlich anerkannten Sachverständigen) von der Normerfüllung akzeptabel ist.
Ein Vergleich der verschiedenen Verkehrsträger Straße, Schiene und Luft (s. Tab. 2.1) verdeutlicht, dass der Grad der Erfüllung einiger Norm-Abschnitte schon allein aufgrund der sehr unterschiedlichen charakteristischen Eigenschaften der den Verkehrsträger nutzenden Verkehrsmittel differenziert betrachtet werden muss und branchenspezifischer Verifizierungen bedarf. Hierfür werden im Folgenden einige ausgewählte Beispiele erläutert.
Während Luftfahrzeuge sich, einmal abgesehen von Bewegungen auf dem Flugfeld, im 3-D-Raum bewegen, ist die Bewegungsfreiheit eines Automobils bereits um einen Freiheitsgrad eingeschränkt, so dass dieses sich nur noch auf der Ebene bewegen kann. Dem Triebfahrzeugführer eines Schienenfahrzeuges wird durch die Schienen-

Tabelle 2.1: Verkehrsträger im Vergleich [SBS08]

	Luftfahrt	**Automobiltechnik**	**Eisenbahntechnik**
			
Bewegung	3-D (Raum)	2-D (Fläche)	1-D (Linie)
Pilot / Fahrer	i. d. R. 2 (Profis)	1 (Amateur v Profi)	1 (Profi [+ Sicherheitsfahrschaltung (Sifa)])
Wetter	Allwetter, ohne Sicht	Allwetter, mit Sicht	Allwetter, ohne Sicht
Phasen	Start, Steig-, Reise, Sinkflug, Landung	Stadt, Autobahn, Landstraße, Parken	Bahnhof, freie Strecke
Stückzahlen (in Europa)	10^3 (Tendenz fallend)	10^6 (Tendenz steigend)	10^3 (Tendenz fallend)
Kosten (Elektronik)	ca. 10.000 €/kg	ca. 1.000 €/kg	ca. 1600 €/kg (z.B. PZB 90; 25000€/15kg)
Frequenz der Modellwechsel	ca. 20 Jahre	ca. 7 Jahre	ca. 40 Jahre
Unfalluntersuchungen	Sehr aufwändig aber meist gut dokumentiert	Wenig aufwändig	Sehr aufwändig, Dokumentation wird besser
Instandhaltung, Reparatur	Nur von zugelassenen Betrieben	Auch kleine „Klitschen“, jeder	auch kleine Werkstätte bei NE-Bahnen

bindung ein weiterer Freiheitsgrad entzogen, so dass dieser sein Fahrzeug nur noch auf einer vorgegebenen Trajektorie führen kann.

Des Weiteren werden erhebliche Unterschiede hinsichtlich der Ausbildung der das Verkehrsmittel führenden Personen deutlich. Der Pkw-Führerschein ist heute schon in gut zwei Wochen zu erwerben, während die Ausbildung zum Triebfahrzeugführer in der Regel etwa sieben Monate dauert. Die Ausbildung zum Piloten dauert etwa noch dreimal so lang.

Gut nachvollziehbar wird die Forderung nach branchenspezifischen Unterschieden in zulassungsrelevanten Normen auch vor dem Hintergrund der die zur Verfügung stehenden Entwicklungszeit stark beeinflussendenden Frequenz des Modellwechsels in den verschiedenen Verkehrsmodi.

In Tabelle 2.1 sind einige weitere charakteristische Eigenschaften enthalten, auf welche hier im Detail nicht näher eingegangen wird.

Bis heute kann bzw. muss ein Automobilhersteller den notwendigen Beweis liefern, allen Erfordernissen bei der Herstellung sicherheitsrelevanter elektronischer Einrichtungen entsprochen zu haben, indem er aufzeigt, dass das Fahrzeug auf allen Ebenen, also auch bei Zulieferern, gemäß den Anforderungen nach IEC 61508 entwickelt und hergestellt wird. Diese, bis zur endgültigen Verabschiedung der ISO 26262 zu-

mindest aus Sicht der Produkthaftung anzuwendende, bewusst generisch gehaltene Norm ist, wie aufgezeigt wurde, jedoch wenig automobilspezifisch und daher nicht in allen Phasen sinnvoll anwendbar.

ISO 26262

Um der im vorherigen Abschnitt beschriebenen fehlenden Automobilspezifizität der IEC 61508 zu entkommen, gibt es im Automobilbereich seit einiger Zeit Bestrebungen die Entwicklung von sicherheitsrelevanter Hard- und Software zu standardisieren.
So wurden Mitte der 90er Jahre von der MISRA Entwicklungsrichtlinien erarbeitet, um erste Standardisierungsversuche in Bezug auf die Entwicklung sicherer Software im Automobilbereich zu starten. Diese Richtlinien werden bis heute ergänzt bzw. überarbeitet und verfolgen vor allem das Ziel, die durch Missverständnisse zwischen Systementwicklern verursachten, strukturellen Schwächen in der Software entgegenzuwirken. Hierfür wurde eine Liste von über 100 Programmierregeln entwickelt, welche fehlervermeidende Maßnahmen im Sinne der IEC 61508 unterstützt.
Darauf aufbauend wird im Rahmen des FAKRA AK 16 Funktionssicherheit („FuSi“), eine sektorspezifische Adaption der IEC 61508 für den Automobilbereich erarbeitet, um die Vereinheitlichung von die Sicherheit beeinflussenden Entwicklungsaktivitäten voranzutreiben. Dieser auf akzeptierten Referenzmodellen der IEC 61508 basierende Normentwurf beschreibt einen automobilspezifischen Sicherheitslebenszyklus und liefert einen automobilspezifischen Ansatz zur Ermittlung von Risikoklassen. Des Weiteren enthält er spezifische Anforderungen zur Softwareentwicklung, und Anforderungen an solch übergreifende Aktivitäten wie die Zertifizierung von Entwicklungswerkzeugen.
Obwohl es sich bei der ISO 26262 zunächst nur um eine sektorspezifische Adaption der IEC 61508 handelt, wurde zu einem gewissen Umfang auch rein strukturell von der Mutternorm Abstand genommen (vgl. Abb. 2.3 und Abb. 2.4), um den Anforderungen des Automobilwesens besser zu genügen. So werden dem Anwender der ISO 26262 bereits in Teil 1 (vgl. IEC 61508 Teil 4) die in sämtlichen Teilen der Norm verwendeten Begriffe und Definitionen an die Hand gegeben.
Teil 2 beschreibt ausführlich die Grundlagen zum Management der funktionalen Sicherheit. Diesem sehr bedeutenden Aspekt wurde im Rahmen der IEC 61508 nur unzureichend Beachtung geschenkt.

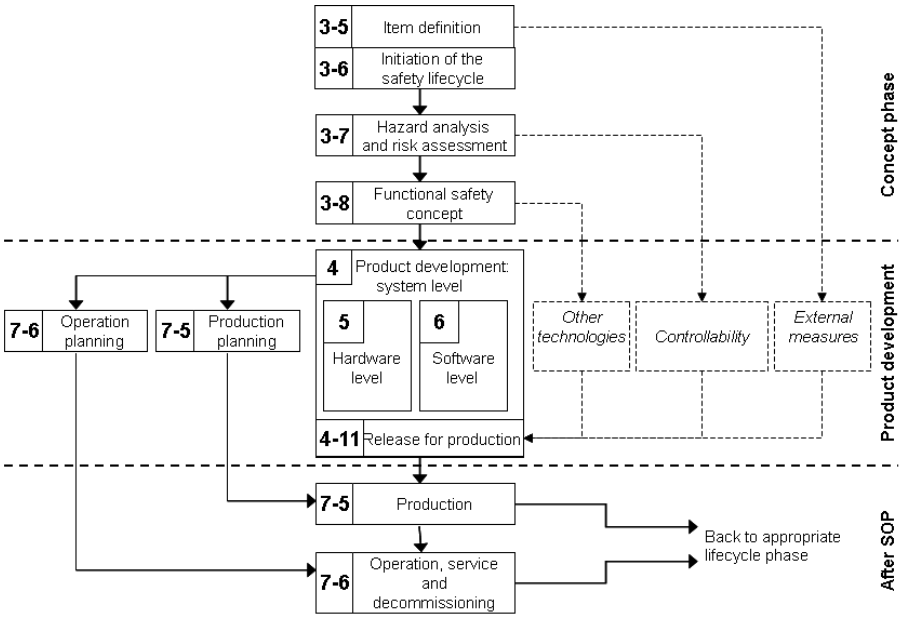


Abbildung 2.4: Sicherheitslebenszyklus nach ISO 26262

Die Teile 3 - 7 beschreiben den eigentlichen Kernprozess der Norm. Teil 3 enthält Anforderungen welche im Rahmen der Konzeptphase (vgl. IEC 61508 Teil 1) der Entwicklung zu erfüllen sind.
Ein wesentlicher Bestandteil dieser Konzeptphase ist die „Gefährdungsanalyse und Risikobewertung“, deren Objektivierung das Ziel dieser Arbeit darstellt.
Die nachfolgenden Teile beschreiben die Produkt-Entwicklungsaktivitäten auf System- (Teil 4), Hardware- (Teil 5) und Software-Ebene (Teil 6), deren analoge Inhalte generisch in den Teilen 2 und 3 der IEC 61508 zu finden sind. Im siebten Teil der Norm wird speziell auf die Produktion und den Betrieb (vlg. IEC 61508 Teil 1) von sicherheitsrelevanten E/E/PE-Systemen in Fahrzeugen eingegangen.
Teil 8 der Norm ist mit „Unterstützende Prozesse“ überschrieben und enthält allgemeine Anforderungen an z.B. die Sicherheitsanalyse und die Gesamt-Dokumentation.
In Teil 9 werden dem Anwender der Norm Vorgehensweisen zur ASIL-Dekomposition aufgezeigt.
Teil 10 stellt einen Anwendungsleitfaden der gesamten Norm dar.
Der Norm-Entwurf wurde im November 2005 mit dem Ziel der Standardisierung als Working Draft (ISO/WD 26262) an die ISO übergeben. Nachdem die Normungsorganisation in 2009 einen inhaltlichen Konsens erreicht hat, ist der Norm-Entwurf derzeit als Draft International Standard (DIS) verfügbar und wird einer öffentlichen

Umfrage unterzogen. Eine endgültige Verabschiedung des ISO 26262 wird für 2011 erwartet [Kri09].

Kapitel 3

Traditionell angewandte Techniken

Zweck dieses Kapitels ist es den Fundus der im Bereich Sicherheits- und Zuverlässigkeitsanalyse zur Verfügung stehenden *Beschreibungsmittel und Methoden*, im Folgenden häufig unter dem Begriff *Technik(en)* subsummiert, strukturiert darzustellen, so dass anschließend (vgl. Kapitel 4) eine anforderungsgetriebene und wissenschaftlich fundierte Auswahl, der der Zielerreichung förderlichsten Technik getroffen werden kann.
Zur einheitlichen Darstellung, und damit zur besseren Vergleichbarkeit der unterschiedlichen Techniken wurde folgende Struktur gewählt, welche den nachstehenden Abschnitten hinterlegt ist.

- **Ziel und Anwendungsbereich(e) der Technik**
  - Welches Ziel wird mit dem Einsatz dieser Technik verfolgt?
  - In welchen Anwendungsbereichen wird die Technik eingesetzt?

- **Historische Entwicklung (informativ)**
  - Seit wann wird die Technik zur Behandlung von technischen Fragestellungen verwendet?
  - Welche Personen werden häufig mit der Technik in Verbindung gebracht?
  - Welche Branche(n) bedient/bedienen sich dieser Technik?
- **Theorie**
  - Welche Theorie steckt hinter dieser Technik?
- **Ansatz**
  - Wie wird bei der Anwendung der Technik vorgegangen?
- **Vor- und Nachteile**
  - Tabellarische Zusammenstellung wesentlicher identifzierter Vor- und Nachteile der Technik.

3.1 Techniken auf Basis statischer Modelle

Die im Bereich Sicherheits- und Zuverlässigkeitsanalyse angewendeten Techniken lassen sich nach [Sch99b] insbesondere hinsichtlich ihrer Fähigkeit unterscheiden dynamisches Verhalten abbilden zu können.
Die in Abschnitt 3.1 dargestellten Techniken, sind in ihrer *„Ur"form*, d.h. ohne eine Kopplung mit anderen Techniken, ausschließlich zur Behandlung von statischen Problemstellungen geeignet.
In Abschnitt 3.2 werden zwei auf zyklischen Graphen basierende Techniken vorgestellt, welche sowohl zur Analyse von statischen als auch dynamischen Prozessen eingesetzt werden können.

3.1.1 Hazard and Operability Study (HAZOP)

Die Hazard and Operability Analysis (HAZOP) ist ein qualitatives Verfahren zur Identifzierung und Analyse von Gefährdungen und betrieblichen Eigenschaften (z.B. zwecks Effizienzsteigerung [Lev01]) von Systemen.
Es handelt sich um eine strukturierte Methode mittels welcher Gefährdungen in

sämtlichen Zwischenstufen von der Konzeptphase bis hin zur Außerbetriebnahme ermittelt werden können. Hierbei liegt das Hauptaugenmerk auf Gefährdungen, welche aus identifizierten potenziellen Abweichungen vom ordnungsgemäßen Betrieb der Betrachtungseinheit resultieren.
Die HAZOP-Analyse kann auf alle Arten von Systemen und ihre unterlagerten Teilsysteme, Bauteile und Komponenten angewendet werden und Umgebungsbedingungen und menschliche Fehlhandlungen in die Analyse mit einbeziehen [Eri05]. Ein wesentlicher Anspruch der Methode ist es, das die Analyse durchführende Team in seiner Kreativität hinsichtlich der Gefährdungsidentifikaktion und der Ermittlung von betrieblichen Problemen zu unterstützen [Lev01].
Die in der IEC 61882 [IEC61882] international standardisierte HAZOP-Analyse wurde in den frühen siebziger Jahren für Chemieanlagen entwickelt und in den frühen neunziger Jahren zur Anwendung auf Software erweitert [Eri05]. Seit einigen Jahren ist der Grundgedanke der HAZOP-Analyse nach [WML05] auch in der Automobilindustrie wiederzufinden.
Der methodische Ansatz der HAZOP-Analyse besteht darin, ein System oder einen Prozess von einem interdisziplinären Team in einer Reihe von Brainstorming-Sitzungen zu analysieren. Das Systemdesign wird mittels verschiedener, aus Leitwörtern (z.B. „kein“, „mehr“, „zuviel“ etc.) und Systemvariablen (z.B. „Temperatur“, „Druck“, „Zeit“ etc.) kombinierter, Fragestellungen kritisch hinterfragt [Lev01]. Ziel des strukturierten Einsatzes dieser Leitwörter ist es zum einen, zu gewährleisten, dass das betrachtete System möglichst vollständig untersucht wird, zum anderen aber auch, den im HAZOP-Team mitarbeitenden Experten aus den unterschiedlichsten Bereichen eine einheitliche begriffliche Basis (s. hierzu auch Kapitel 5) an die Hand zu geben [Eri05].
Tabelle 3.1 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von HAZOP-Analysen.
Abschließend werden einige Hinweise gegeben welche Probleme bei der Durchführung von HAZOP-Analysen auftreten können.
Bei der Durchführung einer HAZOP-Analyse ist stets darauf zu achten, dass aufgrund der ausschließlichen Einfachfehler-Betrachtung nie alle Systemgefährdungen identifiziert werden können, da Gefährdungen häufig eine Folge von mehreren Fehlern sind. Aus diesem Grund bietet es sich an die Methode mit anderen Verfahren zur Gefährdungsidentifikation zu kombinieren [Eri05].

Tabelle 3.1: Vor- und Nachteile von HAZOP [Eri05]

Vorteile	**Nachteile**
- einfach in der Durchführung und im Verständnis - zur Durchführung der Analyse ist kein besonderes Expertenwissen erforderlich - kommerzielle Software ist erhältlich - sehr gängig, weit verbreitet und international standardisiert	- HAZOP-Analysen zielen nur auf Einfachfehler ab; Kombinationen von Ereignissen werden nicht betrachtet - die HAZOP-Analyse kann nur Gefährdungen aufdecken, welche in Relation zu den definierten Leitwörtern stehen; von den Leitwörtern unabhängige Gefährdungen werden leicht übersehen

3.1.2 Fehlermöglichkeits- und Einflussanalyse (FMEA)

Die Fehlermöglichkeits- und Einflussanalyse (engl. Failure Mode and Effects Analysis (FMEA)), auch bekannt als Ausfall-Effekt-Analyse oder Ausfallarten-Auswirkungs-Analyse, ist eine Methode mittels welcher die Auswirkungen bestimmter Fehlermodi von Subsystemen, Bauteilen und Komponenten oder Funktionen frühzeitig erkannt und bewertet werden können.
Sie basiert auf einer textuellen Beschreibung der kausalen Zusammenhänge zwischen Gefahrensituationen, Gefährdungen und technischen Ursachen in tabellarischer Form [Slo06].
Im Gegensatz zur Fehlerbaum-Analyse (FTA) (s. Abschnitt 3.1.4) ist die FMEA eine induktive Methode, die von bekannten Ursachen auf potenzielle Auswirkungen schließt. Eine FMEA setzt beim Wissen über mögliche Fehlermodi einzelner Betrachtungseinheiten an und berücksichtigt die Auswirkungen jedes einzelnen Fehlers auf Subsysteme und auf das Gesamtsystem. Eine häufig eingesetzte Erweiterung der FMEA ist die Fehler-Möglichkeits-Einfluss- und Kritikalitätsanalyse (engl. Failure Mode, Effects and Criticality Analysis (FMECA)), welche über die Berechnung einer Risikopriorität szahl (RPZ) eine detailliertere Betrachtung der Kritikalität und

der Entdeckungswahrscheinlichkeit von potenziellen Fehlermodi ermöglicht [Eri05]. Sowohl FMEA also auch FMECA sind strukturierte und standardisierte bottom-up Methoden, die es ermöglichen, potenzielle Fehler bei der Entwicklung eines Produktes bereits während der Planung bzw. im Systementwurf aufzudecken und diesen mittels geeigneter Maßnahmen entgegenzuwirken [MBKA99, IEC61508]. Das Verfahren wird vorwiegend hardware- oder prozessorientiert angewandt, kann aber gleichermaßen zur Bewertung von Software-Funktionen eingesetzt werden [Eri05].
Die FME(C)A wurde 1949 als formale Analysetechnik zur Bewertung von fehlerabhängigen Zuverlässigkeitseigenschaften für das amerikanische Militär entwickelt und im MIL-P-1629 (heute MIL-STD-1629A) „Procedures for Performing a Failure Mode, Effects and Criticality Analysis“ veröffentlicht. Von dieser Zeit an wurde die Methode zunächst für die Entwicklung von Luftfahrtsystemen, insbesondere aber für die Entwicklung von sehr kostenintensiven kleinen Margen von Raketensystemen, eingesetzt. In den 1960er Jahren wurde die Anwendung von FMEAs im Bereich der Raumfahrttechnik verstärkt, bis sie dann in den 1970er Jahren auch in den Automobilbereich – stark voran getrieben durch Ford – Einzug erhielt. Von nun an wurde die Methode FME(C)A immer weiter standardisiert. Im amerikanischen Raum konnte sich hier insbesondere die SAE J-1739 (2002), im europäischen Raum die IEC 60812 (2006) [DIN60812] durchsetzen.
Die FME(C)A ist ein Verfahren zur qualitativen und quantitativen Bewertung potenzieller Fehlermodi. Mit ihr können nach [Eri05] folgende Problemstellungen bzw. Fragestellungen analysiert werden:

- Wo können Fehler auftreten?
- Wie macht sich dieser Fehler bemerkbar?
- Wie häufig wird der Fehler auftreten?
- Was sind die Auswirkungen dieses Fehlers?
- Welche Auswirkungen auf die Zuverlässigkeit/Sicherheit hat dieser Fehler?

Zu Beginn einer FMEA/FME(C)A ist das zu betrachtende System, der Prozess oder die Funktion in seine Basis-Elemente (z.B. Komponenten) aufzuteilen. Die Basis-Elemente werden in einem FMEA-Formblatt gelistet und individuell analysisert, indem ihnen in einem ersten Schritt Soll-Funktionen zugewiesen werden.

Anschließend werden potenzielle Fehlfunktionen und deren Auswirkungen identifiziert und dokumentiert. Im nächsten Schritt gilt es die potenziell auftretenden Fehler hinsichtlich ihres Risikopotenzials zu bewerten, bevor abschließend eine Systemoptimierung stattfinden kann.
Tabelle 3.2 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von Fehlermöglichkeits- und Einflussanalysen.

Tabelle 3.2: Vor- und Nachteile bei FMEA [Eri05, Bra05]

Vorteile	**Nachteile**
- einfach in der Durchführung und im Verständnis - verhältnismäßig kostengünstig in der Durchführung, aber trotzdem aussagekräftige Ergebnisse - kommerzielle Software ist erhältlich - sehr gängig, weit verbreitet und international standardisiert - aufgrund der hohen Softwarekosten für Spezial-Software ist es positiv zu bewerten, dass die FMEA auch mittels Standardtools (wie MS Excel) durchgeführt werden kann	- es können lediglich Einfachfehler betrachtet werden - menschliche Fehlhandlungen, externe Einflüsse und Schnittstellen können nur begrenzt in die Analyse mit einbezogen werden - im Vergleich zu anderen Verfahren (z.B. FTA) eher unsystematisch

Abschließend werden einige Hinweise gegeben welche Probleme bei der Durchführung von Fehlermöglichkeits- und Einflussanalysen auftreten können. Bei der Anwendung einer FME(C)A ist darauf zu achten, dass aufgrund der ausschließlichen Einfehler-Betrachtung nie alle Systemgefährdungen identifiziert werden können, da

Gefährdungen häufig eine Folge von mehreren Fehlern sind. Aus diesem Grund wird häufig gefordert, dass eine FMEA als induktive Methode nicht eigenständig zur Gefährdungsidentifikation, sondern vielmehr in Kombination mit einer deduktiven Methode (z.B. FTA (s. Abschnitt 3.1.4)), eingesetzt wird.
Des Weiteren darf insbesondere bei der Durchführung einer FMECA nicht außer Acht gelassen werden, dass die die Risikoprioritätszahl bestimmenden Faktoren auf rein subjektiven Schätzungen (s. hierzu auch Abschnitt 1.3.2) basieren und damit Schwankungen unterliegen.
Wird z.B. angenommen, dass die Risikozahlen aufgrund der Subjektivität der Schätzenden um ± 1 varieren, so ergibt sich für ein wahres Risiko von 5 für Auftretenswahrscheinlichkeit, Bedeutung und Entdeckungswahrscheinlichkeit eine Bandbreite von $64 (= 4 * 4 * 4)$ bis $216 (= 6 * 6 * 6)$ für die Risikoprioritätszahl (RPZ) [Pfe01].
Hieraus ergeben sich vor dem Hintergrund der häufig zitierten RPZ-Grenze (vgl. z.B. [Sys06]) von $125 (= 5 * 5 * 5)$ vollkommen unterschiedliche Konsequenzen. So wird bei einer RPZ von 64 voraussichtlich keinerlei weiterführende Maßnahme in Betracht gezogen. Eine RPZ von 216 dagegen visualisiert einen gesteigerten Handlungsbedarf.

3.1.3 Ereignisbaumanalyse (ETA)

Ist im Rahmen einer Sicherheitsanalyse die Abfolge von Ereignissen von Interesse, welche, durch ein Initialereignis ausgelöst, zu einem potenziellen Schadensereignis führen kann, so kann dieser Problemstellung mit einer Ereignisbaumanalyse (engl. Event Tree Analysis (ETA)) begegnet werden.
Für die Durchführung einer ETA werden logische Strukturen, welche zu verschiedenen Ereignissen führen, in einem sog. Ereignisbaum (engl. Event Tree (ET)) induktiv abgebildet und analysisert. Ziel einer ETA ist es zu ermitteln, ob das Auftreten eines Initialereignisses gezwungenermaßen zu einem Schadensereignis führt, oder aber das Schadensausmaß mittels der im System-Design implementierten Sicherungsmaßnahmen und -prozeduren reduziert bzw. sogar verhindert werden kann. Die ETA ist in diesem Zusammenhang ein sehr wirkungsvolles Verfahren, um sämtliche durch ein Initialereignis ausgelösten Ereignispfade (z.B. safe-operation-path, degraded-operation-path oder unsafe-operation-path) zu identifizieren und hinsichtlich ihrer Eintrittswahrscheinlichkeit auszuwerten.
Ereignisbaumanalysen können auf oberster Gesamtsystemebene durchgeführt werden, wodurch Teilsysteme, Bauteile und Komponenten, Software, Prozesse, Umge-

bungsbedingungen und menschliche Fehlhandlungen mit abgedeckt werden [Eri05]. Ereignisbaumanalysen können besonders effektiv in folgenden Anwendungsbereichen eingesetzt werden. Zum einen zur Identifikation und Optimierung von Schutzeinrichtungen, welche aufgrund ihrer (Un-)Wirksamkeit einen überproportionalen Einfluss auf die Eintrittswahrscheinlichkeit eines bestimmten Schadensereignisses haben. Zum anderen sind Ereignisbaumanalysen sehr gut dafür geeignet *Top Level Events* (TLEs) für anschließende Fehlerbaumanalysen (s. Abschnitt 3.1.4) zu bestimmen. Außerdem werden Ereignisbäume dazu verwendet verschiedene Unfallszenarien darzustellen, welche aus einem einzigen Initialereignis resultieren können.
Die Ereignisbaumanalyse wurde erstmals in den frühen 70er Jahren im Rahmen der WASH-1400 Studie zur Analayse der Sicherheit von Kernkraftanlagen angewendet. Die WASH-Arbeitsgruppe versuchte damals einen Fehlerbaum für Kernkraftreaktoren zu erstellen, welcher zur Berechnung der Eintrittswahrscheinlichkeit des Top Level Events „durch Unfall verursachter Austritt von Radioaktivität“ dienen sollte. Hierbei musste die Arbeitsgruppe feststellen, dass diese Fehlerbaummodellierung zu nahezu unendlich komplizierten Strukturen führte. Dies bewog sie dazu ihre sehr komplexe Problemstellung mittels eines in den Bereichen der Geschäfts- und Wirtschaftlichkeitsanalyse weit verbreiteten Verfahrens, der Analyse von Entscheidungsbäumen, in mehrere kleine Problemstellungen zu unterteilen. Hierauf basierend wurde dieser Formalismus der Analyse von Entscheidungsbäumen für technische Systeme unter dem Begriff der Ereignisbaumanalyse weiter verbreitet. Die Ereignisbaumanalyse wird bis heute in sehr vielen Bereichen (z.B. Kernkrafttechnik, Raumfahrttechnik, Chemieanlagenbau) erfolgreich angewendet [Lev01].
Die Ereignisbaumanalyse ist in in DIN 25419 [DIN25419] national normiert. Zur Zeit wird eine internationale Norm IEC 62502 [DIN62502] erarbeitet, welche sich im Stadium *Committee Draft* befindet.
Die Ereignisbaumanalyse wird verwendet, um ausgehend von einem Initialereignis vorwärtsgerichtet verschiedene resultierende Ereignisse in Abhängigkeit von implementierten bzw. geplanten Schutzeinrichtungen zu identifizieren. Hierfür werden implementierte bzw. geplante Schutzeinrichtungen von links nach rechts, die Reihenfolge ist ausschlaggebend, aufgelistet. Im Folgenden wird der Ereignisbaum gleichermaßen von links nach rechts konstruiert. Hierbei wird i.d.R. unter jeder Schutzeinrichtung eine einfache Verzweigung modelliert, weswegen das Ergebnis einer ETA als binärer Raum dargestellt werden kann. Unterschieden wird jeweils zwischen

Wirksamkeit und Unwirksamkeit der betrachteten Schutzeinrichtung. Nachdem diese Baumstruktur entwickelt ist, können die verschiedenen Pfade verfolgt werden, welche zu einem gefährlichen Ereignis führen. Die Eintrittswahrscheinlickeit eines jeden gefährlichen Ereignisses kann durch Multiplikation der Wahrscheinlichkeiten der verschiedenen Verzweigungen des zum Ereignis führenden Pfades berechnet werden [Lev01].
Tabelle 3.3 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von Ereignisbaum-Analysen.
Abschließend werden einige Hinweise gegeben welche Probleme bei der Durchfüh-

Tabelle 3.3: Vor- und Nachteile von Ereignisbaum-Analysen [Eri05, Har08]

Vorteile	**Nachteile**
- sehr strukturierter methodischer Ansatz - ein großer Teil der Arbeit kann computergestützt erfolgen - einfach zu erlernen, anzuwenden und zu verstehen - sehr komplexe Zusammenhänge können verständlich dargestellt werden - kombiniert Hardware, Software, Umgebung und menschliche Interaktion - erlaubt eine Wahrscheinlichkeitsbewertung - kommerzielle Software ist erhältlich	- Ereignisbaumanalyse geht stets von einem einzigen Initialereignis aus, weswegen eine Vielzahl von ETAs erforderlich sind, wenn die Konsequenzen von mehreren Initialereignissen bestimmt werden sollen - aufgrund der Verdopplung der Pfade nach jedem Zwischenereignis und in Abhängigkeit von der Systemgröße kann ein Ereignisbaum sehr komplex werden

rung von Ereignisbaum-Analysen auftreten können.
Die am häufigsten auftrenden Fehler bei der Durchführung von Ereignisbaumanalysen sind nach [Eri05] sowohl die Identifikation von für die Analyse ungeeigneten Initialereignissen als auch eine unvollständige Identifikation der entscheidenden zentralen Ereignisse.

3.1.4 Fehler- oder Störungsbaumanalyse (FTA)

Ziel einer Fehlerbaumanalyse (engl. Fault Tree Analysis (FTA)), auch bekannt als Störungsbaumanalyse oder Ausfallbedeutungs-Analyse, ist es, mögliche Kombinationen von (Basis-)Ursachen zu bestimmen, welche zu bestimmten unerwünschten Ereignissen, den sogenannten *Top Level Events* (TLEs), führen können. Als deduktive Technik geht die FTA, wie sie in der IEC 61025 [DIN61025] international standardisiert ist, von bekannten Auswirkungen aus und ermittelt sukzessiv die zugrunde liegenden unbekannten (Basis-)Ursachen. Hieraus wird deutlich, dass die Fehlerbaumanalyse vornehmlich ein Mittel zur Analyse von Gefährdungen auslösenden Ursachen ist, nicht aber ein Werkzeug um Gefährdungen zu identifizieren [Lev01].
Der tatsächlichen Fehlerbaumanalyse vorgeschaltet ist die Modellierung des sogenannten Fehlerbaums (engl. Fault Tree (FT)). Unter einem Fehlerbaum wird ein Modell verstanden, welches die verschiedenen logischen Kombinationen von möglichen Ereignissen – sowohl fehlerhafter, als auch ordnungsgemäßer Ereignisse – graphisch repräsentiert, welche zu unerwünschten Systemzuständen oder -ereignissen führen können.
FTA finden im Wesentlichen in folgenden zwei Themenfeldern Anwendung. Am weitesten verbreitet ist die proaktiv eingesetzte FTA. Hierbei geht es um die Durchführung und Auswertung von Fehlerbäumen mit dem Hintergrund ein qualitativ hochwertiges und sicheres System zu entwickeln und das Design basierend auf den durchgeführten Analysen positiv zu beeinflussen. Diese Art der FTA kann in allen Phasen vom Konzept bis hin zum Betrieb eines Systems angewendet werden. Besonders effektiv wird die proaktive FTA eingesetzt, um verschiedene Systemkonzepte objektiv zu beurteilen und zu einem hinsichtlich dem Ausfallverhalten optimierten System-Design zu gelangen [BL04].
Reaktiv werden FTA durchgeführt, um Unfallhergänge oder Ereignisketten, welche

zu Beinaheunfällen geführt haben, zu rekonstruieren.
Sowohl die proaktive als auch die reaktive FTA kann drei wesentliche Ergebnisse liefern. Zum einen kann die Auftretenswahrscheinlichkeit eines unerwünschten Ereignisses, zum anderen aber auch die Signifikanz von verschiedenen fehlerbehafteten Ereignissen (cut sets), welche zum unerwünschten Ereignis führen, berechnet werden. Außerdem kann mittels einer Fehlerbaumanalyse die Importanz der unterschiedlichen Basisursachen bestimmt werden [Eri05].
Die Fehlerbaumanalyse wurde erstmals im Jahre 1961 von H.A. Watson im Bereich der Telekommunikations-Technik eingesetzt. Die erfolgreiche Anwendung animierte Ingenieure des Flugzeugbauers Boeing die Methode weiterzuentwickeln und anzuwenden. Einen mindestens ebenso großen Zuspruch brachten der FTA Experten für Sicherheitsanalysen von Kernkraftwerken entgegen [Eri05].
Mit einfachen Fehlerbäumen können die verschiedenen Kombinationen von Ereignissen, welche zu einem TLE führen, analysiert werden. Bei der Modellierung von zeitabhängigem Verhalten stößt diese Art der Modellierung an ihre Grenzen [Bra05]. Daher werden im Rahmen der FT-Erstellung die Bedingungen die zu TLEs führen i.d.R. zu unspezifisch modelliert. Im Allgemeinen führt dies zur Herleitung von Risiken, wie sie so in der Realität nicht gegeben sind. Diese und andere Limitationen führen zu einer kontinuierlichen Weiterentwicklung der Methode, um den rein statischen konventionellen Ansatz um die Möglichkeit der Modellierung der Dynamik relevanter Ereignisse zu erweitern.
Eine aktuelle Erweiterung von Fehlerbäumen stellen die am Fraunhofer Institut für Experimentelles Software-Engineering entwickelten State/Event Fault Trees (SEFT) dar [KGF07]. Diese Strukturen erlauben es explizit zwischen Zuständen und Zustandsübergängen – hierfür sind im Fehlerbaum Petrinetz-Strukturen (vgl. Abschnitt 3.2.2) hinterlegt – zu unterscheiden. In der Folge können temporale Beziehungen zwischen den auslösenden Grundereignissen spezifiziert und so für das TLE ein im Allgemeinen niedrigeres, der Realität eher entsprechendes Risiko berechnet [KLM03] werden.
Als ein weiterer aktueller Ansatz sollen an dieser Stelle auch parametrisierte Störungsbäume genannt sein, wie sie in [BFGP03] beschrieben sind. In diesen werden identische Einheiten gefaltet und indiziert, so dass lediglich ein Repräsentant einer solchen Einheit im Modell aufgenommen wird. Parametrisierte Störungsbäume werden meist zur Analyse redundant ausgelegter Systeme eingesetzt.

Im Folgenden soll kurz auf die der Fehlerbaumanalyse zugrundeliegende Theorie eingegangen werden. Die Analyse erfolgt Top-Down und dient wie oben beschrieben der Identifzierung der Ursachen eines unerwünschten Ereignisses auf oberster Ebene (TLE) [Bra05]. Hierbei beschreibt nach [Lev01] jede Ebene einen identischen Sachverhalt, welcher bis hin zur Komponenten-Ebene immer weiter detailliert wird. Sämtliche zwischen dem TLE und den Basis-Ereignissen (z.B. Komponentenausfällen) modellierten Ereignisse stellen sog. Pseudo-Ereignisse, also Abstraktionen von realen Ereignissen, dar. Diese ergeben sich durch beliebige Kombinationen von Basis-Ereignissen und spielen i.d.R. für die formale Analyse der Baumstrukturen eine untergeordnete Rolle.
Nachdem der Fehlerbaum konstruiert ist, kann dieser in einen Booleschen Ausdruck umgewandelt werden. Dieser kann soweit vereinfacht werden, dass die relevanten, das TLE verursachenden, Kombinationen von Ereignissen abzulesen sind. Ist des Weiteren eine quantitative Analyse gewünscht, kann die Auftretenswahrscheinlichkeit des TLE berechnet werden.
Tabelle 3.4 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von Fehlerbaum-Analysen.
Abschließend werden einige Hinweise gegeben welche Probleme bei der Durchführung von Fehlerbaum-Analysen auftreten können.
Bei der Durchführung einer FTA sollte darauf geachtet werden, dass bestimmte weit verbreitete Fehler vermieden werden, da diese die ansonsten oben als Vorteile beschriebenen Eigenschaften hinfällig erscheinen lassen. So ist stets zu beachten, dass zur Durchführung der FTA ein sehr umfangreiches Verständnis des System-Designs und -betriebs erforderlich ist. Des Weiteren muss darauf geachtet werden, dass neben den technischen Komponentenfehlern oder -ausfällen auch Fehlhandlungen des Betriebspersonals – auch wenn für diese keine gesicherten Ereignisdaten vorliegen [Lev01] – in die Modellierung integriert werden. Um sowohl Modell als auch Analyse verständlich zu gestalten ist eine ordentliche Benennung der einzelnen Knoten des Fehlerbaums unumgänglich [Eri05].

3.2 Techniken auf Basis zyklischer Graphen

Die in den Abschnitten 3.1.1 bis 3.1.4 beschriebenen Techniken sind nicht ohne Weiteres geeignet, um ein dynamisches Systemverhalten darzustellen. Hierzu bedarf es

Tabelle 3.4: Vor- und Nachteile von Fehlerbaumanalysen [Eri05, Bra05, Mah00]

Vorteile	**Nachteile**
- sehr strukturierter methodischer Ansatz - verhältnismäßig einfach zu erlernen, anzuwenden und zu verstehen - kombiniert Hardware, Software, Umgebung und menschliche Interaktion - kommerzielle Software ist erhältlich - eine weit verbreitete und vielfach eingesetzte und über viele Jahre bewährte Technik - international standardisiert - die flussdiagrammähnliche graphische Darstellung ermöglicht es systemseitige Zusammenhänge detailliert darzustellen, wodurch Rückschlüsse auf konzeptionelle Defizite erleichtert werden	- im Gegensatz zu zustandsraumorientierten Analysemethoden handelt es sich bei der Fehlerbaumanalyse um eine statische Analyse; es kann nur ein Systemzustand zu einem bestimmten „eingefrorenem“ Zeitpunkt analysiert werden - stochastische Abhängigkeiten, wie beispielsweise gemeinsame Reparatureinheiten für verschiedene Komponenten oder beschränkte Ersatzteilressourcen sind mittels der Fehlerbaumanalyse nicht modellierbar

einer Technik welche nicht nur statische Zustände, sondern insbesondere auch Zustandsübergänge im System abbilden kann. Auf eben solche, auf zyklischen Graphen basierende Techniken wird in den nachstehenden Abschnitten eingegangen.

3.2.1 Markov-Modelle (MK)

Markov-Analysen (MA) können zur Bestimmung der Eintrittswahrscheinlichkeit von globalen Systemzuständen herangezogen werden. Hierfür werden Systemzustände und Zustandsübergangsbedingungen modelliert und darauf basierend die Eintrittswahrscheinlichkeit des jeweils interessierenden Zustandes berechnet. Mittels MA können Systemstrukturen, einschließlich zeitlichem Verhalten, Reihenfolge, Reparatur, Redundanz und Fehlertoleranz [Eri05, MBKA99], abgebildet werden.
Die Anwendung auf sehr umfangreiche Systeme ist eher kritisch, da Zustandsautomaten bei einer großen Anzahl von Zustandsvariablen aufgrund ihres Umfangs oft nicht mehr handhabbar sind (*Zustandsraumexplosion* [Mah00]).
Markov-Ketten sind Zufallsprozesse, in welchen Zustandsänderungen immer nach festgelegten Zeitabständen auftreten. Die Zukunft des Systems hängt nur von der Gegenwart – nach [Cho99] also von der Zustandswahrscheinlichkeit des aktuellen Zustandes und der aktuellen Zustandsübergangswahrscheinlichkeit – und nicht von der Vergangenheit ab („Gedächtnislosigkeit“), weswegen nur Systeme behandelt werden können, deren Elemente konstante Ausfall- und Reparaturraten besitzen [BL04]. Trotz dieser Einschränkungen können mittels Markov-Ketten eine Vielzahl von in der Realität auftretenden physikalischen Phänomenen (z.B. Komponentenausfälle, radioaktiver Zerfall etc.) abgebildet werden.
MA werden sehr häufig im Rahmen von Leistungs-, Verfügbarkeits-, Zuverlässigkeits- und Sicherheitsanalysen von Systemen eingesetzt [Eri05]. Ziel ist hier unabhängig vom Anwendungsbereich die Berechnung der Wahrscheinlichkeit eines beliebigen Systemzustandes.
Die Theorie der Markov-Ketten ist auf den russischen Mathematiker Andrei A. Markov (1856-1922), ein Schüler des Mathematikers Tschebytscheff, zurükzuführen. Sie basiert insbesondere auf Markovs systematischen Untersuchungen der Möglichkeit Zufallsprozesse mathematisch zu beschreiben. Die Anwendung der Markov-Analyse bzw. des Markov-Verfahrens ist in IEC 61165 [DIN61165] international standardisiert.

Markov-Analysen basieren auf einem einzigen Zustandsübergangs-Diagramm, welches sowohl betriebliche Zustände als auch Fehlzustände des Systems abbildet. Ein Zustandsübergangs-Diagramm, bestehend aus Zuständen (Kreisen), Zustandsübergängen (Pfeilen) und Übergangsraten, kann hierbei sowohl für einzelne Komponenten als auch für ein Gesamtsystem entwickelt werden.
Bei der Konstruktion des Zustandsübergangs-Diagramms sind im Wesentlichen folgende Schritte abzuarbeiten. Ausgehend von einem globalen Initialzustand (alle Komponenten sind i.O.) werden die Konsequenzen einzelner Komponentenausfälle untersucht. Aufgrund dieser Komponentenausfälle, symbolisiert durch mit Ausfallraten versehene Transitions-Pfeile, ergeben sich neue Gobalzustände. Dieses Prozedere wird wiederholt bis sämtliche die Systemfunktion realisierenden Komponenten ausgefallen sind. Es ist stets darauf zu achten, ob ein weiterer Komponentenausfall in einem bereits zuvor definierten Systemzustand mündet.
Der Markov-Prozess ist vollständig durch die Matrix der Transitions-Wahrscheinlichkeiten, welche aus dem Zustandsübergangs-Diagrammm abgeleitet werden kann, charakterisiert.
Im Falle von Sicherheits- oder Zuverlässigkeitsanalysen wird im Markov-Modell sowohl der Komponenten-Ausfall als auch die Komponenten-Reparatur in die Betrachtung mit einbezogen. Die Übergangswahrscheinlichkeiten zwischen den verschiedenen Zuständen lassen sich als eine Funktion der Ausfall- und Reparaturraten der unterschiedlichen Systemkomponenten ausdrücken. Auf diese Weise lässt sich ein Satz von Differentialgleichungen 1. Ordnung (Anzahl der DGL 1. Ordnung = Anzahl der Zustände) ableiten, welcher den Markov-Prozess vollständig beschreibt.
Tabelle 3.5 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von Markov-Modellen.
Abschließend werden einige Hinweise gegeben welche Probleme bei der Anwendung von Markov-Modellen auftreten können. Auch im Rahmen der Durchführung einer Markov-Analyse sollte darauf geachtet werden verbreitete Fehlanwendungen zu vermeiden. Ein sehr häufig anzutreffender Fehler ist hierbei, dass das „komplizierte“ Markov-Verfahren angewendet wird, obwohl z.B mit der „einfachen“ Fehlerbaumanalyse (vgl. Abschnitt 3.1.4) ebenfalls adäquate Ergebnisse erreicht werden können. Ein weiterer schwerwiegender Fehler ist es eine Problemstellung mittels Markov-Analyse anzugehen, obwohl z.B. das Ausfallverhalten bestimmter Systemkomponenten nachweislich nicht konstant ist.

Tabelle 3.5: Vor- und Nachteile von Markov-Modellen [Eri05, Bra05, Slo06, KGF07]

Vorteile	**Nachteile**
- zeitliches Verhalten, Reihenfolge, Reparatur, Redundanz und Fehlertoleranz können modelliert und analysiert werden - MA ist gut geeignet, um das betriebliche Verhalten, Fehlerzustände und Reparatureigenschaften von Systemen zu verstehen - weit verbreitete und standardisierte Methode	- Markov-Modell wird sehr schnell groß/unübersichtlich („Zustandsraumexplosion“), weswegen die Anwendung eher auf kleinere Systeme beschränkt ist - Beschränkung auf konstante Ausfall- und Reparaturraten (neg. Exponentialverteilung); „Gedächtnislosigkeit“ - es können nur globale Systemzustände modelliert werden, weswegen praktische Anwendbarkeit auf komplexe Systeme, deren Design während des Entwurfsprozesses häufig iterativ geändert wird, nicht gegeben ist - es existiert kein allgemeingültiges Verfahren zur Modularisierung von Markov-Modellen, wodurch Modelle schnell unübersichtlich und nicht mehr handhabbar werden - erhöhter Einarbeitungsbedarf für den Anwender

3.2.2 Petrinetze (PN)

Petrinetze sind bipartite Graphen zwischen deren Objekten, den Stellen, Transitionen und Marken Multirelationen bestehen, welche aufgrund ihrer formalen Basis zur Abbildung und Analyse von dynamischem Systemverhalten geeignet sind [Sch99b, ISO15909, Rei85].
Die Analyse von Petrinetzen (eng. Petri net analysis (PNA)) kann besonders effektiv zur Identifzierung von Gefährdungen in zeit- oder reihenfolgeabhängigen Systemen mit oder ohne Reparatur von Komponenten eingesetzt werden [Sch99a]. Des Weiteren kann mittels Petrinetz-Modellierung Leistungs- und Verlässlichkeitsverhalten modelliert und auf den Modellen basierend die Erreichbarkeit von Zuständen (z.B. gefährliche Zustände) analysiert werden.
Ziel der Petrinetz-Modellierung ist es, Systemkomponenten auf hohem Abstraktionsniveau graphisch zu modellieren, um Aussagen bezüglich der Systemzuverlässigkeit und -sicherheit zu erhalten. Die gewonnenen graphischen Modelle können in einem mathematischen Modell zur Berechnung der Eintrittswahrscheinlichkeit von beliebigen Zuständen verwendet werden.
Ein wesentlicher Unterschied zwischen Petrinetzen und den in Abschnitt 3.2.1 beschriebenen Markov-Ketten ist, dass bei der Petrinetzmodellierung zwischen lokalen und globalen Zuständen unterschieden werden kann. Ein globaler Zustand definiert sich hier aus der Menge der lokalen Zustände, womit auch der Lokalität von Zustandsänderungen Rechnung getragen wird.
Eine lange Tradition haben Petrinetze auf dem Gebiet der Beschreibung der Systemzuverlässigkeit (s. z.B. [DTGN84]), die insbesondere in jüngster Zeit mit den Arbeiten von Trost und Slovak (PROFUND-Ansatz) erfolgreich weitergeführt wurden (vgl. [Tro08, Slo06]).
Grundsätzlich lassen sich Petrinetze in unzähligen Anwendungsgebieten (z.B. Abbildung von Geschäftsvorgängen, betrieblichen Organisationsstrukturen, Instanzenwegen, Automatenbedienungen, Bauanleitungen etc.) einsetzen [Bau96]. Besonders gut bewährt haben sie sich neben der Systemzuverlässigkeit auch bei der Beschreibung von dynamischen Systemen in den Bereichen der Leit-, Fertigungs-, Verfahrens-, Kommunikations- und Verkehrstechnik [Cho99, Zim08].
Petrinetze wurden erstmals 1962 von Carl Adam Petri in seiner Dissertation *Kom-*

munikation von Automaten [Pet62] definiert. Darauf aufbauend konnte ihre Theorie weiterentwicklt – z.B. Kopplung von Fehlerbäumen mit Petrinetzen etc. – und erfolgreich in den verschiedensten technischen Bereichen angewendet werden [Eri05, Sch99a]. Im Unterschied zu den übrigen in der Zuverlässigkeitsanalyse Anwendung findenden Techniken haben Petrinetze ihren Ursprung also in der Wissenschaft und diffundieren allmählich in die Industrie. Mit dem Erscheinen der ISO 15909 [ISO15909] ist die Anwendung der Petrinetzmodellierung seit 2004 international genormt. Ein speziell auf die Anwendung von Petrinetzen zur Analyse der Zuverlässigkeit von Systemen abzielender Standard (DIN EN 62551) [IEC62551] befindet sich derzeit abschließenden Normungsstadium.
Petrinetze können sowohl zur rein grafischen als auch zur mathematischen Modellierung von Systemen (s. hierzu auch die verschiedenen Petrinetztypen in Abschnitt 4.3.1), Prozessen o.ä. verwendet werden. Durch die beiden dualen Elemente Plätze (Kreise) und Transitionen (Balken, Rechtecke) werden lokale Zustände und Zustandsübergänge dargestellt. Gerichtete Kanten (Pfeile) zwischen Plätzen und Transitionen modellieren die logisch-dynamische Verknüpfung zwischen Zustandskombinationen als Bedingung für einen Zustandsübergang und der resultierenden Folgezustände. Durch Markierung von Plätzen kann im Sinne eines Markenspiels unter Beachtung verschiedener Schaltregeln die Ablaufdynamik im Netz veranschaulicht werden („Tokengame“) [VDI3682, VDI4009].
Tabelle 3.6 gibt einen Überblick über die wesentlichen in der Literatur aufgezeigten Vor- und Nachteile von Petrinetz-Modellen.
Abschließend werden einige Hinweise gegeben welche Probleme bei der Anwendung einer Petrinetz-Analyse auftreten können. Auch im Rahmen der Durchführung einer Petrinetz-Analyse muss darauf geachtet werden verbreitete Fehlanwendungen zu vermeiden. Ein sehr häufig anzutreffender Fehler ist hierbei, dass das „komplizierte“ Petrinetz-Verfahren angewendet wird, obwohl z.B mit der „einfachen“ Fehlerbaumanalyse ebenfalls adäquate Ergebnisse erreicht werden könnten.

3.3 Ergänzende Techniken

Im Zuge der Auswahl einer geeigneten Technik zur Objektivierung von Schätzaufgaben, werden neben den bisher im Detail vorgestellten noch zwei weitere in Betracht gezogen, welche im Folgenden aber begründet nicht näher analysiert werden. Die

Tabelle 3.6: Vor- und Nachteile von Petrinetz-Modellen [Eri05, Slo06, VDI3682, Har08]

Vorteile	**Nachteile**
- Petrinetze können zur übersichtlichen Modellierung auf unterschiedlichen Abstraktionsleveln (Konzept- bis Feindesignphase) verwendet werden - Zeitliches Verhalten, Reihenfolge, Reparatur, Redundanz und Fehlertoleranz abbildbar - in den Transitionen lassen sich beliebige stochastische Verteilungsfunktionen hinterlegen - Petrinetze basieren auf einer präzisen mathematischen Grundlage, die hohe Anforderungen an spezielle Analyseeigenschaften erfüllt - hierarchische Strukturen abbildbar - Entwurfsveränderungen sind verhältnismäßig leicht anpassbar - Unterscheidung zwischen globalen und lokalen Zuständen	- Petrinetze sind nicht für jeden Betrachter intuitiv zu verstehen; erhöhter Einarbeitungsbedarf für den Anwender - bisher keine ausgereifte Toolunterstützung - trotz der genannten Vorteile noch Akzeptanzprobleme

Argumentation hierfür wird in den nachstehenden Abschnitten erbracht.

3.3.1 Zuverlässigkeitsblockdiagramme (RBD)

Zuverlässigkeitsblockdiagramme (engl. Reliability Block Diagrams (RBD)) stellen eine in der Sicherheits- und Zuverlässigkeitsanalyse weitverbreitete und anerkannte Technik dar [Lig00, IEC61078].
Auf eine detaillierte Betrachtung dieses Beschreibungsmittels wird im Zuge dieser Arbeit verzichtet, da sich jede mittels RBD darstellbare Problemstellung ohne großen Aufwand in eine Fehlerbaumstruktur (vgl. Abschnitt 3.1.4) überführen lässt und die Ergebnisse direkt voneinander abhängig sind [JBAW05, Bir07]. So wird mittels einer Fehlerbaumanalyse die Ausfallwahrscheinlichkeit $F(T)$ und unter Verwendung von Zuverlässigkeitsblockdiagrammen die Überlebenswahrscheinlichkeit $R(t)$ bestimmt, welche nach Formel 3.1 direkt komplementär sind.

$$F(t) = 1 - R(t) \tag{3.1}$$

3.3.2 Entscheidungstabellen (ET)

Im Zuge der Auswahl von Techniken zur Objektivierung von Schätzaufgaben wird, neben den traditionellen Ansätzen der Zuverlässigkeits- und Sicherheitsanalyse, auch der Einsatz der eher im strukturierten Software-Entwurf verbreiteten, und in DIN 66241 genormten, Entscheidungstabelle in Betracht gezogen. Dies insbesondere vor dem Hintergrund, dass sich diese formale Methode durch Stringenz und Übersichtlichkeit auszeichnet, wenn es darum geht Entscheidungsregeln auf logische Richtigkeit, d.h. Konsistenz inklusive Widerspruchsfreiheit und insbesondere Vollständigkeit zu überprüfen [Sch99b].
Von der Anwendung dieser Vorgehensweise wird jedoch im Hinblick auf die Tatsache, dass dynamische Strukturen, die über eine einfache Iteration hinausgehen – hierunter fallen sich verändernde Fahrszenarien – nicht ausgedrückt werden können, Abstand genommen [Ern08].
Auf eine detaillierte Vorstellung dieser im Bereich der Zuverlässigkeits- und Sicherheitsanalyse ohnehin wenig verbreiteten Vorgehensweise wird hier aus den genannten Gründen verzichtet. Ein guter Überblick über die Einsatzmöglichkeiten, aber auch über Vor- und Nachteile von Entscheidungstabellen wird in [Ern08] gegeben.

3.4 Zusammenfassung des Technik-Überblicks

Um der in Abschnitt 1.1 motivierten Problemstellung zu begegnen bedarf es der Nutzung einer geeigneten Technik welche einen Beitrag zur Objektivierung von Schätzungen leisten kann.
Welche Technik in diesem Kontext am zielführendsten eingesetzt werden kann, ist nicht ohne Weiteres zu beurteilen. So findet in der Praxis eine so große Anzahl von unterschiedlichen Verfahren zur Gefährdungs- bzw. Risikoanalyse Anwendung, dass laut [Eri05, Lev01] das größte Problem häufig in der Auswahl einer geeigneten Technik liegt, welche auf dem Weg zur eigentlichen Problemlösungsfindung am effektivsten eingesetzt werden kann.
Da jede der Techniken wie oben gezeigt ihre Vor- und Nachteile aufweist und zudem nur in bestimmten Phasen der Entwicklung (vgl. Abb. 3.1) gewinnbringend eingesetzt werden kann, ist häufig der Einsatz einer Kombination von Techniken (z.B. FMEA und FTA) in Erwägung zu ziehen.

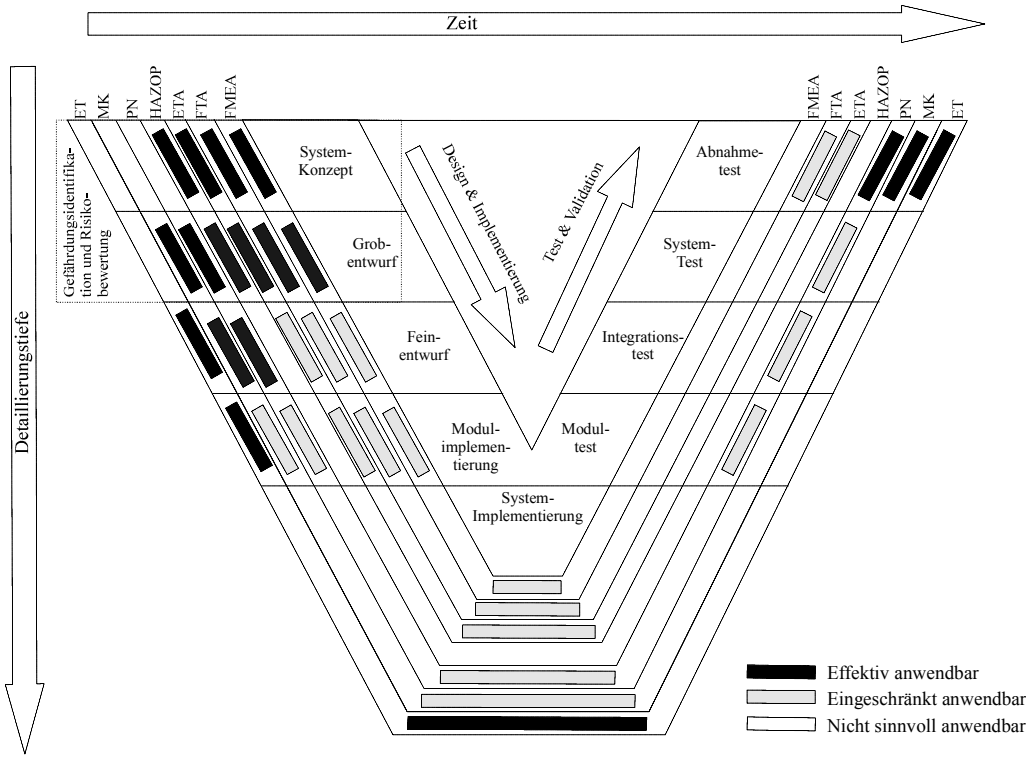


Abbildung 3.1: Phasenzuordnung der betrachteten Techniken

Ziel von Kapitel 3 ist es potenziell zur Problemlösung zur Verfügung stehende Techniken aus dem Bereich der Sicherheits- und Zuverlässigkeits-Analyse vorzustellen.
In diesem Abschnitt erfolgt nun unter Verwendung von Tabelle 3.7 eine grobe Klassifikation bzw. Einordnung der dargestellten Techniken.

Tabelle 3.7: Grobklassifzierung der Techniken

Technik	**B/M**[a)]		**Kriterium**[b)]								**Entwicklungs-Phase**[c)]						
	Beschreibungsmittel (B)	Methode (M)	Formale Basis	Verhaltensbeschreibung	Struktur	Expertise	Standardisierung	Akzeptanz und Anwendbarkeit	Explizite Zeitdarstellung	Prozess-Interaktionen	Anforderungsanalyse/Konzept	Grobdesgin	Feindesign	Modul-Implementierung	Systemintegration	Testen	Abnahme und Betrieb
Hazop and Operability Study (HAZOP)	-	X	-	0	0	0	+	+	-	-	+	-	-	-	-	-	-
Fehlermöglichkeits- und Einflussanalyse (FMEA)	-	X	-	0	0	0	+	+	-	0	+	+	0	-	-	-	-
Ereignisbaumanalyse (ETA)	X	X	+	+	+	0	+	+	-	0	+	+	+	-	-	-	0
Fehlerbaumanalyse (FTA)	X	X	+	+	+	0	+	+	-	-	+	+	0	-	-	-	0
Markov-Modell	X	-	+	+	0	+	+	0	+	-	+	+	+	0	-	+	0
Petrinetz	X	-	+	+	+	+	+	0	+	+	+	+	+	+	-	+	0
Zuverlässigkeitsblockdiagramme (RBD)	X	-	+	+	+	0	+	+	-	-	+	+	0	-	-	-	0
Entscheidungstabellen	X	X	+	0	-	+	+	0	-	-	-	+	+	+	-	+	0

a) Ein "X" weist darauf hin, dass die Technik dieser Spalte zugewiesen wird, andernfalls wird die Spalte mit einem "-" gekennzeichnet.

b) "+": die Technik erfüllt das Kriterium vollständig
"0": die Technik erfüllt das Kriterium eingeschränkt
"-": die Technik erfüllt das Kriterium nicht

c) "+": die Technik kann in der Phase sinnvoll eingesetzt werden
"0": die Technik kann in der Phase eingeschränkt eingesetzt werden

Die Tabelle ist wie folgt arrangiert. Die einzelnen Zeilen der Tabelle werden durch die in den Abschnitten 3.1 bis 3.3 vorgestellten Techniken aufgespannt. Die einzelnen Spalten sind in folgende drei Gruppen zusammengefasst:

- B/M: Diese Spalte dient dazu eine Technik als Beschreibungsmittel, Methode oder als integrierte Methode (Eigenschaften von Beschreibungsmittel und Methode) zu klassifzieren.
- KRITERIUM: In den einzelnen Spalten finden sich eine Reihe von Kriterien wieder, welche der Charakterisierung der unterschiedlichen Techniken dienen. Die

einzelnen Kriterien, deren Erfüllungsgrad mit den nachstehend aufgeführten Hilfs-Fragen geprüft werden kann, sind:

- Formale Basis: Besitzt die Technik eine mathematische Basis und eine definierte vollständige Syntax sowie eine eindeutige semantische Interpretation?
- Verhaltensbeschreibung: Kann die Technik zur Beschreibung von dynamischem Systemverhalten verwendet werden?
- Struktur: Kann die Technik zur Beschreibung von Systemstrukturen (z.B. Hierarchie, Komposition/Dekomposition) verwendet werden?
- Expertise: Sind spezielle Fähigkeiten/Vorkenntnisse erforderlich, um die Technik anzuwenden?
- Standardisierung: Existieren Normen, Standards oder anerkannte Richtlininen, welche die Anwendung der Technik erläutern?
- Akzeptanz und Anwendbarkeit: Wird die Technik in der jeweiligen Branche akzeptiert und angewendet?
- Explizite Zeitdarstellung: Bietet die Technik dem Anwender die Möglichkeit quantitative Aussagen zu Zeitpunkten und Zeitdauern (z.B. zwischen Ereignissen) zu modellieren?
- Prozessinteraktion: Kann die Technik zur Beschreibung bzw. Analyse von synchronen, asynchronen oder nebenläufigen Prozessen genutzt werden?

- Entwicklungsphase: In dieser Spalte können die unterschiedlichen Techniken einzelnen oder mehreren Entwicklungsphasen zugeordenet werden, in denen sie sinnvoll eingesetzt werden können.

Sowohl Abbildung 3.1 als auch Tabelle 3.7 bestätigen die in der Einleitung dieses zusammenfassenden Abschnitts angedeutete Problematik, dass keine Technik uneingeschränkt in den verschiedenen Entwicklungsphasen eingesetzt werden kann.
Wird der Blick auf die sehr frühen Phasen des Entwicklungsprozesses, also insbesondere die Konzept- und Anforderungsphase, in der auch die Risikoanalyse enthalten ist, fokussiert, wird die in Abschnitt 3.3.2 getroffene Entscheidung der Nichtverfolgung der Entscheidungstabellen bestätigt. Gleichermaßen wird deutlich, dass theoretisch alle übrigen Techniken gewinnbringend zur Durchführung von Risikoanalysen

eingesetzt werden können.
Inwiefern sie auch einer Objektivierung der Einschätzung des Automotive Safety Integrity Levels dienlich sein können wird in Abschnitt 4 im Detail auf Basis eines anforderungsgetriebenen *paarweisen Vergleiches* analysiert.

Kapitel 4

Anforderungsgetriebene Auswahl der EmMORI-Technik

In Kapitel 3 werden eine Reihe von Beschreibungsmitteln und Methoden vorgestellt, welche in den verschiedenen Branchen im Rahmen der Durchführung von Sicherheits- und Risikoanalysen (z.B. FMEA, HAZOP etc.) zum Einsatz kommen. Ergänzt werden diese durch Techniken, wie sie im artverwandten, sehr umfangreichen Themengebiet der Technischen Zuverlässigkeit (z.B. Petrinetze, Markov-Ketten etc.) angewendet werden. Diese Liste der im Bereich Risiko- und Zuverlässigkeitsmanagement anwendbaren Techniken lässt sich nach [Eri05] fast beliebig fortführen. Eines haben alle aufgeführten Techniken gemeinsam. Sie werden in sehr frühen Lebenszyklusphasen zur Analyse von abstrakten *Modellen* angewendet, nicht zur Analyse von realen *Systemen*.
Die Qualität der Analyse-Ergebnisse ist stark von der Qualität des Modells abhängig, welches das reale System abbildet [Lev01]. Um hierfür zu sensibilisieren, werden Analyseergebnisse in der Praxis häufig mit dem Zusatz „AMMIT - Assuming My Model Is True“ gekennzeichnet.
Neben dieser unspezifischen Schwäche der Anwendung von Beschreibungsmitteln und Methoden zur Analyse von realen Systemen wird in Kapitel 3 auf die verschiedenen Vorzüge und Schwächen der Anwendung der verschiedenen Ansätze eingegangen. Diese Zusammenstellung allgemeiner Vor- und Nachteile kann jedoch bei der Auswahl einer für eine Problemlösung geeigneten Technik nur Anhaltspunkte liefern, nicht aber ausschlaggebend sein.
Dieser Umstand ist darin begründet, dass die Vielzahl der Beschreibungsmittel

bzw. Methoden speziell zur Beantwortung einer speziellen Fragestellung entwickelt wurden. Es ist von Anwendungsfall zu Anwendungsfall abzuwägen, inwiefern eine Methoden-Eigenschaft der Beantwortung einer bestimmten Aufgabenstellung förderlich ist oder der Lösungsfindung wenig dienlich ist.
Um aus der für den Einzelnen kaum noch zu überschauenden Vielfalt von Beschreibungsmitteln und Methoden einen zur Beantwortung einer spezifischen Fragestellung geeigneten Lösungsansatz zu identifizieren, wurden in VDI/VDE 3681 [VDI3681] und [Sch99b] eine Reihe von Klassifikationskriterien identifziert, mittels welcher die Eignung von Beschreibungsmitteln und Methoden für spezielle Analysetätigkeiten unterschieden werden kann.
Zur qualitativen Beurteilung der Anwendbarkeit dieser Kriterien wird in [Sch99b] eine an den Entwicklungsphasen orientierte Gewichtung derselben vorgeschlagen. Allerdings wird in [Sch99b] und [CJS98] gleichermaßen darauf hingewiesen, dass die Definition und die allgemeine Akzeptanz von verbindlichen Werten problematisch ist. Diese Problematik ist in hohem Maße auf die unterschiedlichen subjektiven Einschätzungen zurückzuführen (vgl. Abschnitt 5.1.10), die auf differenzierte Gewichtungen verschiedener Merkmale beruhen.
Diesen subjektiven Einflüssen wird im Rahmen dieser Arbeit wie in Abschnitt 4.2 beschrieben mittels des paarweisen Vergleiches entgegengewirkt. Charakteristisch für den paarweisen Vergleich ist, dass nicht jedes Beschreibungsmittel einzeln gegen die Erfüllung von Kriterien geprüft wird. Es wird vielmehr systematisch die Anforderungserfüllung eines jeden Beschreibungsmittels direkt mit der Eignung jedes anderen Beschreibungsmittels verglichen. Hierdurch werden nach [Kau05] persönliche Vorlieben unterbunden, wodurch eine objektivere Entscheidung getroffen werden kann.
Dennoch können die Bewertungskriterien aus [Sch99b] genutzt werden und durch branchenspezifische (in diesem Fall automobilspezifische) Kriterien bzw. Anforderungen an Beschreibungsmittel und Methoden ergänzt werden und in den paarweisen Vergleich einfließen.
Eben auf diese branchenspezifischen Einordnungskriterien wird in Abschnitt 4.1 im Detail eingegangen.

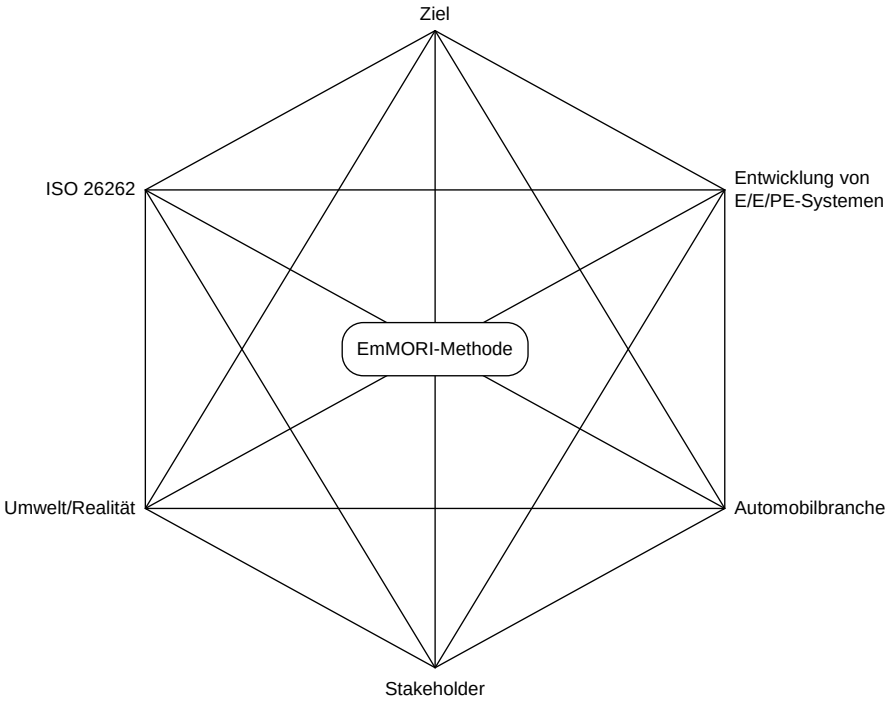


Abbildung 4.1: Die Anforderungen bestimmenden Konstituenten

4.1 Anforderungen an das EmMORI-Beschreibungsmittel

Im vorherigen Absatz ist aufgezeigt, dass zur Bewertung bzw. zum Vergleich der verschiedenen zur Verfügung stehenden Beschreibungsmittel und Methoden geeignete Kriterien definiert und insbesondere auch branchen- bzw. systemspezifische Anforderungen hinzugezogen werden müssen.
Dieser Forderung wird im Folgenden strukturiert nachgekommen. Hierzu werden die Konstituenten (vgl. Abb. 4.1) identifziert, welche einen Einfluss auf die Durchführung der Gefährdungs- und Risikoanalyse haben bzw. spezielle Anforderungen an diese stellen.

Im Rahmen der vorliegenden Arbeit, mit dem darin formulierten Ziel der Objektivierung der Gefährdungs- und Risikoanalyse nach ISO 26262, lassen sich folgende Konstituenten mit ihren abgeleiteten Anforderungen identifizieren:

- ISO 26262
  - fordert als Meta-Anforderung die Durchführung einer *Situationsanalyse*; die Situation charakterisierende Eigenschaften können „nebenläufig“, „sequentiell“ oder kausal abhängig sein

    * fordert die Abbildbarkeit von *Nebenläufigkeit*: z.B. kann eine Fahrsituation durch „hohe Verkehrsdichte“ *und* „schlechte Sichtbedingungen“ *und* „ schlechte Straßenverhältnisse“ gekennzeichnet sein
    * fordert die Abbildbarkeit von *sequentiellen Prozesse*: z.B. Anfahren - Beschleunigen - unbeschleunigtes Fahren - Verzögern - Anhalten
    * fordert die Abbildbarkeit von *kausalen Zusammenhängen*: z.B. bei hoher Verkehrsdichte und schlechten Sichtbedingungen wird i.d.R. mit niedrigeren Geschwindigkeiten gefahren als bei niedriger Verkehrsdichte und guten Sichtbedingungen
    * fordert die Abbildbarkeit von *externen Einflüssen*: z.B. Regen, Nebel etc.

- Formuliertes Ziel dieser Arbeit/Methode
  - fordert ein *formales* simulationsfähiges Modell
  - *Simulation* und *Analyse* fordern *Toolunterstützung*
- Umwelt/Realität
  - vgl. Anforderungen aus Situationsanalyse; die Umweltbedingungen/ Umgebungsbedingungen charakterisieren die Fahrsituation
- Akteure/Stakeholder (Gutachter, Anwender, Entscheider etc.)
  - *Übersichtlichkeit*
  - *Nachvollziehbarkeit* z.B. durch *Objektorientierung*
- Automobilbranche
  - fordert *Einhaltung der geltenden Normen* bzw. der anerkannten Regeln der Technik
- Entwicklung von E/E/PE-Systemen
  - fordert *Anpassungsfähigkeit der Methode an Veränderungen in der Entwicklung*

Da kein Beschreibungsmittel bzw. keine Methode existiert, die sämtlichen Anforderungen in vollem Umfang gerecht wird, wird im Folgenden ein Kriterien-Ranking erstellt, welches verdeutlicht, dass sich die Anforderungen bezüglich ihrer Wichtigkeit deutlich unterscheiden.
Hierfür werden die zur Auswahl stehenden Anforderungen durch paarweise Vergleiche systematisch gegenübergestellt und bewertet. Dabei wird eine komplexe Entscheidung mit all ihren unüberschaubaren Abhängigkeiten und Widersprüchen in eine Reihe leicht durchzuführender paarweiser Vergleiche zerlegt [Dil00].
Hierzu wird jedes Einzelkriterium (A) mit jedem anderen (B) verglichen und deren Wichtigkeit in der direkten Gegenüberstellung festgelegt. Die Entscheidungsmenge wird hierbei auf „A wichtiger B“ ($\rightarrow$ 2), „A und B gleichwichtig“ ($\rightarrow$ 1) und „A unwichtiger B“ ($\rightarrow$ 0) reduziert. Die Summe der Einzelbewertungen führt zu einer Aussage der Gesamtwichtigkeit jedes Einzelkriteriums in Form einer Rangziffer.
Der Hauptnutzen dieser Methode liegt darin, dass durch den direkten Vergleich subjektive Einflüsse unterdrückt werden. Nähere Erläuterungen zur Methode des paarweisen Vergleiches sind u.a. in [Dil00] zu finden.
Der zur Wichtung der Anforderungen an Beschreibungsmittel und/oder Methode angestellte paarweise Vergleich liefert die in Tabelle 4.1 dargestellte Anforderungs-Importanz.
Hiermit wurde die Relevanz folgender Kriterien systematisch aufgezeigt:

1. **Normkonformität**: Den normativen Anforderungen des ISO 26262 darf nicht widersprochen werden. Zudem sollte das verwendete Bescheibungsmittel bzw. die verwendete Methode eine normative Basis haben.

2. **Anpassungs-/Aktualisierbarkeit**: Eine Anpassung des Modells muss bei sich verändernder Struktur/Funktion des zu entwickelnden Systems ohne allzu großen Aufwand in das Modell implementiert werden können.

3. **Simulations- und Analysefähigkeit**: Bei der Untersuchung von Problemstellungen bzw. Systemen, welche ein gewisses Maß an Komplexität überschreiten oder aber durch stochastisches Verhalten charakterisiert sind, stoßen analytische Methoden an ihre Grenzen. In diesem Fall stellt sich die Simulation von realen Problemstellungen bzw. realen Systemen abstrahierenden Modellen (Modellbasiertheit) als eine kostengünstige und reproduzierbare Ergänzung/Alternative zu Theorie und Experiment dar.

Tabelle 4.1: Paarweiser Vergleich zur Anforderungspriorisierung

Anforderung	Nebenläufigkeit	Sequentialität	Kausalität	externe Einflüsse	Anpassungsfhäigkeit	Übersichtlichkeit	Formalität	Hierarchisierung	Toolunterstützung	Normkonformität	Objektorientierung	Simulations- und Analysefähigkeit	Zeilensumme	normierte Zeilensumme (+22)	relative Bedeutung	Rang
Nebenläufigkeit	X	1	1	0	2	0	1	0	1	2	0	1	9	31	0,915	4
Sequentialität	1	X	1	0	2	0	1	0	1	2	0	1	9	31	0,915	4
Kausalität	1	1	X	0	2	0	1	0	1	2	0	1	9	31	0,915	4
externe Einflüsse	2	2	2	X	2	1	1	1	2	2	1	2	18	40	0,891	10
Anpassungs-fähigkeit	0	0	0	0	X	1	1	0	1	1	0	1	5	27	0,926	2
Übersichtlichkeit	2	2	2	1	1	X	2	1	1	2	0	2	16	38	0,896	9
Formalität	1	1	1	1	1	0	X	0	1	2	0	1	9	31	0,915	4
Hierachisierung	2	2	2	1	2	1	2	X	2	2	1	2	19	41	0,888	11
Toolunter-stützung	1	1	1	0	1	1	1	0	X	2	0	1	9	31	0,915	4
Normkonformität	0	0	0	0	1	0	0	0	0	X	0	1	2	24	0,934	1
Objektorient.	2	2	2	1	2	2	2	1	2	2	X	1	19	41	0,888	11
Simulations-/ Analysefähigkeit	1	1	1	0	1	0	1	0	1	1	1	X	8	30	0,918	3

Jedes Spaltenkriterium (A) wird jedem Zeilenkriterium (B) gegenübergestellt und hinsichtlich seiner Importanz bewertet:

$0 \rightarrow$A unwichtiger gegenüber B; $1 \rightarrow$A und B sind gleichwichtig; $2 \rightarrow$A wichtiger gegenüber B

4. **Formale Basis**: Die formale Basis einer Technik nach [VDI3681], also deren mathematische Basis, deren vollständig definierte Syntax sowie deren eindeutige semantische Interpretation, ist eine notwendige Bedingung für die Simulation, Analyse und Verifikation von Prozessen bzw. Systemen. [Sch99b]

5. **Toolunterstützung**: Mit immer komplexer werdenden Aufgabenstellungen ist der Entwicklungsprozess von der Modellierung bis zur Implementierung ohne Einsatz leistungsfähiger Entwicklungswerkzeuge nicht mehr handhabbar. Besonders für die Visualisierung und die Simulation der erstellten Modelle stellen Tools (s. auch Abschnitt 4.4) eine wichtige Voraussetzung dar.

6. **Nebenläufigkeit**: Prozesse heißen nebenläufig, wenn sie voneinander (kausal) unabhängig, jedoch nicht notwendigerweise gleichzeitig ablaufen. [VDI3681]

7. **Sequentialität**: Im Gegensatz zu nebenläufigen Prozessen ist von sequentiellen Prozessen die Rede, wenn deren Ereignisse kausal voneinander abhängig sind. [Sch99b]

8. **Kausalität**: Im Sinne eines kausalen Wirkzusammenhangs können spätere Zustände nur von ihren vorangegangenen abhängig sein. Kausalität wird als Logik von Abläufen verstanden. [Sch99b]

9. **Übersichtlichkeit**: Die zur Modellierung zu verwendenden Symbole sollen einer bestimmten Bedeutung zuzuordnen und für den Anwender leicht zu verstehen sein. Ein besseres Modellverständnis wird insbesondere dann erreicht, wenn die Modelle weitgehend den kognitiven Vorgängen und den mentalen Repräsentationen des Menschen entsprechen [Sch99b]. Des Weiteren kann die Übersichtlichkeit in gewissen Grenzen durch Hierarchisierung[1] von Modellen verbessert werden.

[1] Dem zuvor identifzierte Kriterium der *Hierarchisierung* ($\rightarrow$ *Aktuere/Stakeholder*) wurde auf Basis des paarweisen Vergleiches nur eine niedere Priorität zugewiesen, da sie für sich allein lediglich eines von vielen Stilmitteln zur Verbesserung der *Übersichtlichkeit* ist.

4.2 Paarweiser Vergleich zur Verfügung stehender Techniken

In Abschnitt 4.1 sind die wichtigsten Anforderungen, denen die EmMORI-Technik gerecht werden muss, gelistet. Im Folgenden sind die in Kapitel 3 beschriebenen Beschreibungsmittel und Methoden hinsichtlich des Erfüllungsgrades dieser identifzierten Anforderungen zu bewerten.
Bildlich gesprochen werden hierzu die verschiedenen Beschreibungsmittel in einen „Trichter“ (vgl. Abbildung 4.2) geschüttet. Im Zuge eines „Filtrier-Prozesses“ durch die unterschiedlichen von den identifzierten Anforderungen aufgespannten Sieb-Ebenen wird das am besten geeignete Beschreibungsmittel herausgefiltert.

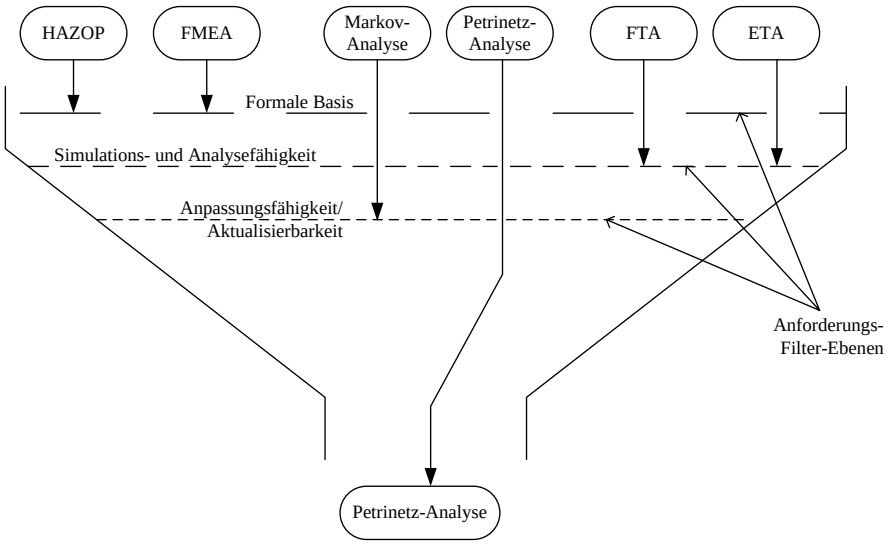


Abbildung 4.2: „Technik-Trichter“ (exemplarisch)

Zur Auflösung der Entscheidungskomplexität bei der Auswahl einer Technik wird wiederum der paarweise Vergleich herangezogen. Die zugehörigen Entscheidungsmatrizen sind dem Anhang A zu entnehmen.

Auf Basis der systematischen Gegenüberstellung der verschiedenen zur Verfügung stehenden Techniken haben sich aufgrund des höchsten Grades der Anforderungserfüllung Petrinetze als geeignetes Beschreibungmittel hervorgetan (s. Tabelle 4.2). Vor dem Hintergrund dieser auf systematischer Analyse der Anforderungs-Erfüllung beruhenden Ergebnisse können die zustandsorientierten, soll heißen sowohl (Global-/

Tabelle 4.2: Paarweiser Vergleich – Gesamtbewertung

Gesamt-Bewertung	Standardisierung/Normkonformität	Anpassungs-/Aktualsierbarkeit	Simulation und Analysefähigkeit	Formalisierungrad	Toolunterstützung	Nebenläufikgkeit	Sequentialität	Kausalität	Übersichtlichkeit	Zeilensumme	Rang
HAZOP	0,86	0,82	0,83	0,82	0,81	0,85	0,83	0,82	0,83	7,45	7
FMEA	0,86	0,87	0,83	0,82	0,87	0,85	0,83	0,87	0,84	7,61	6
ETA	0,86	0,87	0,87	0,87	0,87	0,86	0,90	0,87	0,90	7,85	2
FTA(RBD)	0,86	0,87	0,87	0,87	0,87	0,86	0,87	0,88	0,90	7,83	3
Markov-Modell	0,86	0,87	0,88	0,87	0,87	0,86	0,87	0,85	0,83	7,75	4
Petrinetz	0,86	0,87	0,90	0,87	0,87	0,90	0,90	0,88	0,85	7,90	1
Entscheidungs-tabelle	0,86	0,85	0,84	0,87	0,87	0,83	0,83	0,83	0,85	7,62	5

Lokal-)Zustände und Zustandsübergänge bzw. Ereignisse abbildenden, Petrinetze als geeignetes Beschreibungsmittel für die Objektivierung der Gefährdungs- und Risikoanalyse nach ISO 26262 identifziert werden.
Hiermit wird in den folgenden Kapiteln auf ein in der Automobilindustrie noch wenig verbreitetes, aber, wie nachstehende Beispiele zeigen, nicht völlig unbekanntes Beschreibungsmittel aufgesetzt.
Es ist festzuhalten, dass zustandsorientierte Ansätze in der Automobilindustrie häufig dann zum Einsatz kommen, wenn es darum geht Zustandsautomaten zu implementieren (z.B. auf Autobox). Auch im Bereich der Gefährdungs- und Risikoanalyse ist die Zustandsorientierung keineswegs unbekannt. So wurde beispielsweise in einer dem committee draft vorhergehenden Fassung der ISO CD 26262, in Baseline 10 ein auf einer Markov-Kette beruhendes „Automotive Risk Model“ beschrieben, auf dessen Basis die Eintrittswahrscheinlichkeit verschiedener Systemzustände berechnet werden konnte. Im Draft International Standard der ISO 26262 ist dieses „Automotive Risk Model“ nicht mehr enthalten.
Mahmoud geht in seiner Dissertation [Mah00] sehr detailliert auf die Vorzüge der Kopplung der statischen Fehlerbaum- mit der zustandsorientierten Markov-Analyse im Bereich der Sicherheitsanalyse ein.
Explizite Anwendungsbeispiele von Petrinetzen in der Automobilbranche finden sich im Bereich der Analyse von Kommunikationsarchitekturen für Kraftfahrzeuge [Glä07] und der On-Board-Diagnose [MBS07, SCST08].
Den Beweis, dass Petrinetze gewinnbringend in die frühen Phasen des Entwicklungsprozesses von sicherheitsrelevanten technischen Systemen eingebracht werden können, hat zudem Slovak in [Slo06] am Beispiel komplexer Eisenbahnanlagen erbracht.
Auf Grundlage der hier zusammengestellten Auflistung an Anwendungsbeispielen der Zustandsorientierung im Allgemeinen und der Petrinetze in der Automobilbranche im Besonderen und dem nachgewiesenem Grad der Anforderungserfüllung (vgl. Abschnitt 4.2) wird in den nachfolgenden Kapiteln eine Methode dargestellt, welche auf dem Beschreibungsmittel „Petrinetz“ basiert. Dies auch im Hinblick auf die explizite Benennung der Petrinetze als für Risiko- und Sicherheitsanalysen geeignetes Beschreibungsmittel in der den Stand der Technik zum „Zuverlässigkeitsmanagement“ beschreibenden IEC 60300.

4.3 EmMORI-Technik – Stochastische Petrinetze

Auf Basis des paarweisen Vergleiches der verschiedenen in Kapitel 3 vorgestellten Beschreibungsmittel und -methoden ist aufgezeigt, dass Petrinetze die aus dem Ziel dieser Arbeit hervorgegangenen Anforderungen am besten erfüllen.
Während in Abschnitt 3.2.2 ausführlich auf die geschichtliche Entwicklung, die Hauptanwendungsbereiche und auf Vor- und Nachteile von PN im Allgemeinen eingegangen wird, sollen im Folgenden die theoretischen Grundlagen der unterschiedlichen PN-Typen detaillierter erläutert werden.

4.3.1 Theoretische Grundlagen und Eigenschaften

Petrinetze sind zur Beschreibung des dynamischen Verhaltens eines diskreten Ereignissystems in einer statischen kausal-logischen Struktur geeignet. Hierbei handelt es sich um bipartite gerichtete Graphen (s. Abbildung 4.3). Eine gute Einführung in Petrinetze gibt z.B. [Bau96].

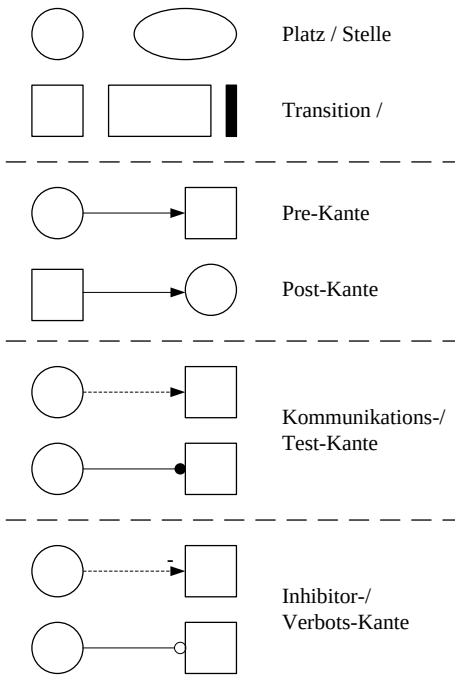


Abbildung 4.3: Symbolik der Petrinetze (allgemein)

Petrinetz-Formalismen gründen sich auf der Dissertation von Petri [Pet62]. Hier wurden die PN zur Beschreibung kommunizierender Automaten entwickelt.
Ganz allgemein werden Petrinetze und deren Verhalten unter Verwendung nachstehender Notationselemente dargestellt [ISO15909, Bau96, Rei85, Fay99, Slo06]:

- *Plätze bzw. Stellen* können als diskrete (einzelne) individuelle stationäre Zustände in einem System aufgefasst werden. Sie haben *Kapazitäten*, die angeben, wie viele Marken sie maximal aufnehmen können.

- *Transitionen* können als diskretes (einzelnes), kurzfristiges Ereignis bzw. als Zustandsübergang eines Systems aufgefasst werden. Sie repräsentieren Aktionen.

- *Kanten* können als Kausalrelationen zwischen Plätzen und Transitionen interpretiert werden. Gerichtete Kanten zwischen Plätzen und Transitionen modellieren die logisch-dynamische Verknüpfung zwischen Zustandskombinationen als Bedingung für einen Zustandsübergang und den resultierenden Folgezuständen [Sch09]. Die Kanten haben ein *Gewicht*, welches angibt, wie viele Marken jeweils auf einmal über diese Kante fließen.

- Grundregel des Aufbaus von Petrinetzen ist, dass Transitionen immer nur mit Stellen und Stellen immer nur mit Transitionen verknüpft werden können.

- *Marken* symbolisieren die aktuell bestehenden Zustände. Ist eine Bedingung zu einem Zeitpunkt erfüllt (lokaler Zustand), so ist der zugehörige Platz markiert. Die Menge der Marken aller zu einem Zeitpunkt erfüllten Bedingungen repräsentiert den globalen Zustand des diskreten Ereignissystems.

- Ist ein Ereignis *aktiviert* (d.h. die Transition ist schaltfähig), werden von den Stellen, von denen eine Kante zu der Transition hinführt, so viele Marken abgezogen, wie die Kantengewichte angeben, und auf den Stellen, zu denen eine Kante von der Transition hinführt, so viele Marken erzeugt, wie die Kantengewichte angeben.

Dieses intuitive Verständnis der Petrinetze ist für die weitere Diskussion ausreichend, weswegen im Rahmen dieser Arbeit auf eine formale Definition von PN nicht näher eingegangen wird.

Der Formalismus eignet sich darüber hinaus zur Beschreibung von Systemen in verschiedensten Anwendungsgebieten mit unterschiedlichen Zielen. Die Zahl der Anwendungen ist inzwischen so groß, dass ein Petrinetz als universeller Formalismus angesehen werden kann und somit der Verweis auf weitere, die in Abschnitt 4.2 aufgeführten Anwendungen, ergänzende Anwendungen nicht erforderlich ist. Die diversen Anforderungen an PN, die sich durch deren unterschiedliche Einsatzmöglichkeiten ergeben, führen nicht selten zur Erweiterung des Formalismus in sogenannte Petrinetz-Typen [Sch99b]. Wesentliche Konzepte dieser Erweiterungen sind Konzepte der Markenindividualisierung (z.B. [GV02], [Bau96], [Rei85]) und Zeitkonzepte. Einige dieser Petrinetztypen werden im Folgenden kurz beschrieben, bevor letztendlich der den Anforderungen am besten genügende Typ ausgewählt wird.

Bedinungs-Ereignis-Netze (B/E-Netze)

Bedingungs-Ereignis-Netze stellen die einfachste Art von Petrinetzen dar. Sie sind dadurch gekennzeichnet, dass sämtliche Plätze die Kapazität 1 und alle Kanten das Gewicht 1 aufweisen. Die Markierung stammt also aus einer zweielementigen Menge $\{0,1\}$.

Stellen-Transitions-Netze (S/T-Netze)

Stellen-Transitions-Netze sind gegenüber den B/E-Netzen eine Verallgemeinerung, da diese Petrinetzklasse erlaubt, dass eine Stelle auch mehrere Marken aufnehmen kann. Dadurch kann die Schaltfähigkeit einer Transition auch von der Anzahl der Marken abhängig gemacht werden, und eine Transition kann beim Schalten mehrere Marken generieren (s. oben: Kantengewicht).

Zeitbehaftete Petrinetze

Während bei einem B/E-Netz die Aktivierung eines Ereignisses als seine Bereitschaft zum Eintreten zu verstehen ist, ist dies in der allgemeinen Petrinetz-Theorie nicht der Fall. Hiernach kann das Ereignis zwar eintreten, muss aber nicht. Um ergänzend die Zeitdauer zwischen Ereignissen modellieren zu können, kann in einem Petrinetz der Zeitbegriff eingeführt werden. Hier wird der Ansatz gewählt den Transitionen Zeitparameter zuzuweisen.
Eine konkrete Klasse der zeitbehafteten Petrinetze bilden Erweiterte Deterministi-

sche und Stochastische Petrinetze (EDSPN - Extended Deterministic and Stochastic Petri Nets) [Ger94, Zim97]. Diese beinhalten sämtliche in der Einführung beschriebenen Notationselemente inklusive verschiedener temporaler Transitionsarten.

Hierarchische Petrinetze

Elementare Petrinetze werden ab einer gewissen Größe unübersichtlich. Daher nutzt man die Möglichkeit, Teile der Netzstruktur zusammenzufassen und in Unternetzen abzulegen. Die Plätze, die Marken in das Unternetz hineinführen, werden als „Input-Port-Places“ und die Plätze, die Marken aus dem Netz herausleiten als „Output-Port-Places“ betitelt. Bei sehr komplexen hierarchischen Strukturen kann es nach [Hör04] sehr aufwendig werden, Unternetze, die durch mehrere Netzebenen getrennt sind, mit Portplätzen zu verbinden. Hier schaffen „Fusion-Places“ Abhilfe, welche beliebig häufig innerhalb der Netzstruktur bzw. innerhalb einzelner Netze angebunden werden können. Wird ein Fusion-Place markiert, steht diese Markierung gleichzeitig in allen Repräsentationen zur Verfügung.

Fuzzy-Petrinetze (FPN)

Im Falle der Fuzzy-Petrinetze werden herkömmliche Petrinetze um Attribute erweitert, die verschiedenen Formen der Ungenauigkeit von Informationen oder Daten Rechnung tragen. Solche Ungenauigkeiten können z.B. auf fehlerhafte oder fehlende Sensordaten oder ungenaue Informationen über Prozessabläufe bzw. Szenarien zurückzuführen sein. Die Integration von Fuzzy-Notationen erlaubt dabei, unscharfes Wissen angemessen zu berücksichtigen [Fay99].

4.3.2 Auswahl des geeigneten Petrinetz-Typs

Im Hinblick auf das in Abschnitt 1.1 formulierte Ziel der Modellierung der schwer fassbaren, den ASIL bestimmenden Parameter könnte man vorschnell zu dem Ergebnis kommen, dass Fuzzy-PN das Beschreibungsmittel der Wahl darstellen. Dies insbesondere vor dem Hintergrund, dass die zu modellierenden die Situationen charakterisierenden Merkmale verschiedenen Arten von Unschärfe („epistemische Unsicherheit“) unterliegen.
Allerdings führt eine Fuzzyfizierung der Problemstellung dazu, dass gerade die aus

zur Verfügung stehenden Statistiken abgeleiteten objektiv(er)en Parameter durch gezielte Verunschärfung erst vage gemacht werden.
Zudem gilt es objektive Unsicherheiten dahingehend zu unterscheiden, ob ihre Quelle in der *Unwissenheit* oder in der *Ungenauigkeit* begründet ist. Denn auch für den Fall, das gewisse Fakten nicht bekannt sind (also Unwissenheit), kann doch zumindest eine Häufigkeitsverteilung (z.B. Nebeltage in Deutschland) dieser Werte gegeben sein, welchen mit den Methoden der *Stochastik* zu begegnen ist.
Ist dagegen davon auszugehen, dass gewisse Daten z.B. aufgrund von (partieller) Unkenntnis über per se nicht zufällige Phänomene unsicherheitsbehaftet sind, so kann möglicherweise die *Fuzzy-Logik* zielführender sein.
Unter Berücksichtigung der zuvor beschriebenen Sachverhalte und nachstehenden Zitats des geistigen Vaters der Fuzzy-Logik L. A. Zadeh wird zur Objektivierung der ASIL-Bestimmung ein auf stochastischen Petrinetzen beruhender Ansatz gewählt, der sich zu Teilen der Gedanken der Fuzzy-Logik bedient.

> „Wie die Komplexität eines Systems anwächst, so nimmt unsere Fähigkeit, präzise und gleichzeitig signifikante Aussagen über sein Verhalten zu treffen, ab, bis zu einer Schwelle, jenseits der Präszision und Signifikanz sich geradezu gegenseitig ausschließen“ (L. A. Zadeh, 1973)

So wird dem, im Zitat angemahnten, Komplexitätszuwachs bei der Modellierung von Systemen im Rahmen der EmMORI-Modellierung mittels geeigneter Zergliederung einer sehr komplexen Schätzaufgabe in eine Vielzahl von einfach(er)en Schätzaufgaben begegnet (vgl. Abschnitt 8.4). Diese Teilschätzungen werden zur Parametrisierung von hierarchischen stochastischen PN, welche sich im Vergleich zu Fuzzy-PN durch eine einfachere Syntax und eine einheitliche Theorie auszeichnen [Sch99b], genutzt.

4.4 Werkzeugunterstützung

Aufgrund der Komplexität und des Umfanges der den ASIL bestimmenden Parameter stoßen analytische Methoden bei der realitätsnahen Abbildung von Szenarien schnell an ihre Grenzen, weswegen Simulationsverfahren zum Einsatz kommen müssen.
Im Zuge der die ASIL-Bestimmung objektivierenden Modellierung und Analyse ist

ein leistungsfähiges Entwicklungswerkzeug unabdingbar. Dies gilt auch für die Visualisierung und Simulation der erstellten Modelle.
Die Toolunterstützung zur praktischen Anwendung der im Rahmen des EmMORI-Ansatzes zum Einsatz kommenden Petrinetze zeigt, wie in [Slo06] dargestellt, bis dato noch einige Schwachstellen auf.
Aus diesem Grunde stützt sich das EmMORI-Konzept auf eine erweiterte Version des am Institut für Verkehrssicherheit und Automatisierungstechnik (iVA) der TU Braunschweig entwickelten, aktuell vom Institute for Quality, Safety and Transporation GmbH (iQST) vertriebenen, π-Tools ab.
π-Tool bietet die Möglichkeit der visualisierten Simulation („Tokengame“) und Analyse von hierarchischen stochastischen Petrinetzen, welche in den vorhergehenden Abschnitten anforderungsgetrieben als Beschreibungsmittel der Wahl identifiziert wurden. Zudem können mit π-Tool im Modell enthaltene Deadlocks identifziert werden. Ein weiterer wesentlicher Vorteil des π-Tool besteht in der Bereitstellung eines „Verteilungseditors“, der es dem Entwickler ermöglicht, in Transitionen verschiedenste stochastische Verteilungen zu hinterlegen.
Die Verwendung einer auf der aktuell erhältlichen Version des π-Tool aufsetzenden Beta-Version verbindet folgende Vorteile.
Zum einen wird auf validierte Algorithmen und Funktionalitäten des zugänglichen Software-Werkzeuges aufgesetzt, welche sich bereits bei der Bearbeitung unterschiedlicher Problemstellungen bewährt haben. Auf der anderen Seite kann die Beta-Version, aufgrund des engen Kontaktes zum Softwareentwickler, noch hinsichtlich neu aufkommender Anforderungen angepasst und um neue Funktionsumfänge ergänzt werden, wodurch eine enorme Flexibilität erreicht werden kann.

4.5 Zusammenfassung – EmMORI-Technik

Der Schwerpunkt von Kapitel 4 liegt in der Auswahl einer geeigneten Technik zur Lösung des in Kapitel 1 motivierten Objektivierungsproblems.
Hierzu werden in Abschnitt 4.1 strukturiert von verschiedenen Konstituenten an die Technik gestellte Anforderungen identifiziert.
In Abschnitt 4.2 wird der Erfüllungsgrad der einzelnen Anforderungen durch die verschiedenen in Kapitel 3 vorgestellten Techniken mittels paarweisem Vergleich untersucht. Aus diesem strukturierten Filtrierprozess gehen die Petrinetze als die

die Anforderungen am besten erfüllende Technik hervor.
Im Folgenden werden die bisherigen Anwendungen von zustandsorientierten Techniken im Allgemeinen und Petrinetzen im Speziellen in der Automobilindustrie dargelegt.
Abschnitt 4.3 verschafft einen kurzen Überblick über die verschiedenen verbreiteten Petrinetz-Typen, bevor in Abschnitt 4.3.2 die Begründung für die Anwendung von stochastischen Petrinetzen erbracht wird.
In Folge der in Kapitel 4 gebrachten Argumentationskette werden hierarchische stochastische Petrinetze als geeignetes Beschreibungsmittel identifziert, um das im Rahmen einer ASIL-Bestimmung vorherrschende Objektivierungsproblem zu lösen.

Kapitel 5

Förderung eines einheitlichen Begriffsverständnisses

Das Lesen dieser Arbeit stellt nach [VG01] eine unidirektionale Kommunikation, also eine Übermittlung von Nachrichten vom Autor (Sender) an einen Leser (Empfänger) dar. Hierbei wird größtenteils die natürliche Sprache als Medium der Kommunikation verwendet. Einige Abschnitte werden zur Verdeutlichung von Sachverhalten durch Abbildungen untermalt.
In [WBJ00] ist beschrieben, dass jede Form der Kommunikation als Prozess einer reziproken Bedeutungskonstruktion aufgefasst werden muss. Dies hat zur Folge, dass in der Praxis oftmals Kommunikationsprobleme vorliegen, die nach [Sch09, Rot10, Sch92] unter anderem auf die in Tabelle 5.1 gelisteten Aspekte zurückzuführen sind.
Unter technisch-wirtschaftlichen Gesichtspunkten können solche Kommunikationsprobleme in Folge begrifflicher Unschärfe und mangelhafter Begriffsbildung finanzielle Verluste verursachen, wenn z.B. Dokumente terminologisch inkonsistent sind und dadurch hervorgerufene Missverständnisse zu explodierenden Fehlleistungskosten führen [Sch09].
Dieser wirtschaftliche Einfluss ist nachvollziehbar, wenn man bedenkt, dass die Kommunikation in einem Unternehmen eine wesentliche Basis einer jeden erfolgreichen Zusammenarbeit darstellt. Wird davon ausgegangen, dass ein Unternehmen an zahlreichen Kommunikationsprozessen (z.B. Kunde - Lieferant, Vorgesetzter - Mitarbeiter, Entwickler - Vertrieb etc.) mit verschiedensten Kommunikationsparteien, deren Begriffsmodelle stark voneinander abweichen können, partizipiert, welche sich alle auf den wirtschaftlichen Erfolg des Unternehmens niederschlagen können, wird

Tabelle 5.1: Kommunikationsbeeinflussende Aspekte

Aspekte	**Beispiele**
Mehrdeutigkeit	Spezifikation = Prozess ODER Spezifikation = Dokument
Widersprüchlichkeit	fault is a result of a failure (IEC 60050) [DIN60050] ODER fault is an abnormal condition that may cause a failure (IEC 61508) [IEC61508]
Begriffliche Unschärfe	Durchschnitt = arithmetisches Mittel ODER Durchschnitt = Median
Domänenspezifizität/ Kontextabhängigkeit	Blinker = visueller Fahrtrichtungsanzeiger an Straßenfahrzeugen ODER Blinker = Kunstköder zum Angeln auf Raubfische

der Bedarf an begriffsbildenden bzw. begriffsstrukturierenden Ansäzten deutlich. Ein aktueller Ansatz um diesen Kommunikationshemmnissen entgegenzuwirken ist in [Sch09] beschrieben. Hier wurde ein softwarebasiertes formalisiertes Terminologiemanagementsystem entwickelt, in welchem die einzelnen Termini mit ihren Bedeutungsbeziehungen abgebildet werden, um einen Beitrag zur Eindeutigkeit des Fachvokabulars zu leisten [Sch09].
Um Kommunikations- bzw. Verständnisproblemen beim Lesen dieser Arbeit entgegen zu wirken und ein einheitliches Begriffsverständnis zu fördern, soll dem Leser, und auch potenziellen Anwendern des später vorgestellten methodischen Ansatzes eine Übersicht immer wiederkehrender Begriffe als Hilfsmittel an die Hand gegeben werden.
Da diese Übersicht insbesondere dem besseren Verständnis der vorliegenden Arbeit dienen soll, wird hierbei von der häufig wiederzufindenden rein alphabetischen Aufzählung der Begrifflichkeiten Abstand genommen. Es wird vielmehr das Ziel verfolgt, die unterschiedlichen, für das Verständnis der Arbeit erforderlichen Begrifflichkeiten

im Gesamtkontext entlang einer thematisch strukturierten Begriffsabfolge (*Storyline*) darzustellen.

5.1 Begriffe im automobilen Kontext

Nachfolgende Abschnitte beschreiben unterschiedliche Aspekte eines automobilspezifischen Entwicklungsprozesses in Fließtext. Hierbei werden verschiedene Begriffe (siehe kursive Begriffe) in ihrem fachlichen Kontext verwendet, welche für ein besseres Verständnis dieser Arbeit von Interesse sind. Anschließend werden die interessierenden Begriffe jeweils wieder aufgegriffen und weitestgehend basierend auf in sicherheitsbezogenen Normen und Standards der Automobiltechnik gegebenen Definitionen definiert (siehe eingerahmte Absätze).

5.1.1 Die Entwicklung von sicheren Straßenfahrzeugen

Das Ziel eines jeden Automobil-Herstellers oder -Zulieferers ist die Entwicklung eines den gesetzlichen Rahmenbedingungen genügenden sicheren (*Sicherheit*) *E/E/PE-Systems* welches seine implementierte *Funktion* in einem Straßenfahrzeug bzw. *Personenkraftwagen* realisiert. Hierzu bedarf es einer strukturierten *Sicherheitsplanung*.

Sicherheit

Sicherheit ist die Freiheit von unvertretbaren Risiken. [IEC61508]

E/E/PE

E/E/PE-Systeme basieren auf elektrischer (E) und/oder elektronischer (E) und/oder programmierbar elektronischer (PE) Technologie. [IEC61508]

System

Ein *System* ist eine Menge von Elementen, die nach einem Entwurf in gegenseitiger Beziehung stehen. Ein Element eines *Systems* kann zugleich ein anderes *System* sein, genannt Teilsystem, welches ein steuerndes oder ein gesteuertes

System sein und Hardware, Software und menschliche Eingriffe beinhalten kann. [IEC61508]

(Sicherheits-)Funktion

Eine *Funktion* ist in allgemeinster Form definiert als die Beziehung zwischen abhängigen (Ziel-) und diese beeinflussenden unabhängigen metrisch skalierbaren (Stell-)Variablen [PS03]. Die *Funktion* im technischen Sinne ist die Eigenschaftsänderung von Eingangs- zu Ausgangsgrößen. [Ste98]
Eine *Sicherheitsfunktion* ist eine Funktion, die von einem sicherheitsbezogenen System ausgeführt wird mit dem Ziel, unter Berücksichtigung eines festgelegten gefährlichen Vorfalls einen sicheren Zustand für das betrachtete System zu erreichen bzw. diesen aufrecht zu erhalten. [in Anlehnung an [IEC61508]]

Personenkraftwagen

Personenkraftwagen sind mehrspurige Fahrzeuge mit mindestens 4 Rädern (vgl. [70/156/EWG]) mit eigenem Antrieb zum vorwiegenden Zwecke der Personenbeförderung. Nach §4 Abs. 4 PBefG [PBefG61] sind sie nach Bauart und Ausstattung zur Beförderung von nicht mehr als 9 Personen (inkl. Fahrzeugführer) bestimmt und dürfen ein Gesamtgewicht von 3,5 t nicht überschreiten.

Sicherheitsplanung

Die *Sicherheitsplanung* umfasst die Planung sämtlicher im Rahmen des Sicherheitslebenszyklus eines Systems zu leistenden Sicherheitsaktivitäten (z.B. Ressourcenplanung, Planung von Verifikation und Validierung von Sicherheitsanforderungen etc.). [ISO26262]

5.1.2 Legislative Rahmenbedingungen

Um diesen gesetzlichen Rahmenbedingungen zu genügen, ist der Hersteller vom Gesetzgeber verpflichtet (vgl. Abschnitt 2.1) sein System unter Einhaltung der *anerkannten Regeln der Technik* (Stand der Technik) zu entwickeln. Dieser ist in verschiedenen *Normen* und *Standards* dokumentiert.

Anerkannte Regeln der Technik

Die *anerkannten Regeln der Technik* stellen eine technische Festlegung dar, die von einer Mehrheit repräsentativer Fachleute als Wiedergabe des Standes der Technik angesehen wird. [DIN45020]

Normen vs. Standards

Eine *Norm* ist ein öffentliches, von einer Interessengruppe in einem Gremium, z.B. dem Deutschen Institut für Normung (DIN), erstelltes Dokument welches anerkannte Regeln der Technik wiederspiegelt.
Ein *Standard* hingegen wird von einem Konsortium definiert. Dafür finden sich wirtschaftlich unabhängige Firmen zusammen, um den von ihnen definierten Standard am Markt durchzusetzen. Sie sind in der Regel urheberrechtlich geschützt. [Jak02]

5.1.3 ISO 26262

Die in Zukunft wahrscheinlich wichtigste Norm im Hinblick auf die Entwicklung von E/E/PES im Automobilsektor ist die *ISO 26262* „Straßenfahrzeuge - *Funktionale Sicherheit*“.

ISO 26262 als Derivat der IEC 61508

Die Norm *ISO 26262* ist ein Derivat der bisher auch zur Entwicklung sicherheitsrelevanter Funktionen in der Automobilindustrie angewendeten Sicherheitsgrundnorm IEC 61508. Die Struktur der ISO 26262 stimmt, bis auf einige automobilspezifische Anforderungen, weitestgehend mit der Struktur ihrer Mutternorm überein.
Inhaltlich zielt die Norm auf sämliche Aktivitäten während des Sicherheitslebenszyklusses von sicherheitsbezogenen E/E/PE-Systemen im Automobil ab, welche eine sicherheitsbezogene Funktion realisieren. [ISO26262]

Funktionale Sicherheit

Funktionale Sicherheit bezeichnet den Teil der Gesamtsicherheit eines Systems, der von der korrekten Funktion der sicherheitsbezogenen (Sub-)Systeme und externer Einrichtungen zur Risikominderung abhängt. [IEC61508]

5.1.4 Anwendung der ISO 26262

In ISO 26262 wird in der *Konzeptphase* des automobilspezifischen *Sicherheitslebenszyklus* die Durchführung einer *Gefährdungsanalyse und Risikobewertung* (engl. Hazard analysis and risk assessment) gefordert, für welche sich in der Alltagssprache der Begriff der *Risikoanalyse* manifestiert hat.

Konzeptphase

Die sehr früh im Entwicklungsprozess verankerte *Konzeptphase* beinhaltet gemäß ISO 26262 Anforderungen an die System-/Funktionsdefinition, die Initiierung eines Sicherheitslebenszyklus, die Gefährdungsanalyse und Risikobewertung und das Erstellen eines funktionalen Sicherheitskonzeptes. [ISO26262]

Sicherheitslebenszyklus

Der *Sicherheitslebenszyklus* umfasst die Gesamtheit der Phasen eines sicherheitsbezogenen Systems vom Konzept bis zur Außerbetriebnahme. [ISO26262]

Gefährdungsanalyse und Risikobewertung

Die *Gefährdungsanalyse* beschreibt einen Prozess zur Identifikation von Gefährdungen und der Analyse ihrer Ursachen sowie der Ableitung von Anforderungen, um die Wahrscheinlichkeit und die Folgen von Gefährdungen auf ein akzeptables Maß zu begrenzen.
Die *Risikobewertung* ist eine Methode mittels welcher die identifzierten vom Betrachtungsgegenstand ausgehende Gefährdungen kategorisiert werden, um Sicherheitsziele zu spezifizieren. [DIN50129, ISO26262]

Risikoanalyse

Die *Risikoanalyse* beschreibt eine iterative analytische Untersuchung und Bewertung von Gefährdungen sowie ihrer Ursachen und Konsequenzen.

5.1.5 Identifikation und Bewertung von Gefährdungen

Ziel der Gefährdungsanalyse und Risikobewertung ist es *Gefährdungen*, welche vom zu entwickelnden E/E/PES ausgehen zu identifzieren und das von ihnen ausgehende *Risiko*(potenzial) zu bewerten

Gefahr vs. Gefährdung

Als *Gefahr* wird nach [DIN FB 144] ein Zustand bezeichnet welcher durch die Anwesenheit von unvertretbaren Risiken charakterisiert ist. Dieser Zustand ist die Voraussetzung für das Eintreten einer *Gefährdung*.
Ein *Gefährdung* wird als das räumliche und zeitliche Zusammentreffen [Noh89, PM85] von bestehenden Rechtsgütern und der existenten Gefahr verstanden. Es handelt sich hierbei um eine physikalische Situation, die potenziell einen Schaden für das Rechtsgut beinhaltet bzw. eine Bedingung, die zu einem Unfall führen kann. [DIN50129]

Risiko

Das *Risiko* ist definiert als die Kombination aus der Wahrscheinlichkeit des Auftretens einer Gefährdung, die einen Schaden verursacht, und dem Ausmaß dieses Schadens. [ISO51]

5.1.6 Das Risiko charakterisierende Faktoren

Das Risiko lässt sich in der vorstehenden Definition begründet als Produkt aus der *Schadenseintrittswahrscheinlichkeit* und dem *Schadensausmaß* (engl. Severity) bzw. der *Konsequenz* berechnen.

Schadenseintrittswahrscheinlichkeit

Die *Schadenseintrittswahrscheinlichkeit* beschreibt die statistische Wahrscheinlichkeit, mit der ein bestimmter Schaden eintritt.

Schadensausmaß/Konsequenz

Das *Schadensausmaß* gemäß [ISO26262] ist eine Größe, welche das Ausmaß eines Schadens quantifiziert, welches sich in einer bestimmten Situation für die beteiligten Individuen ergibt.

5.1.7 Bestimmung der Schadenseintrittswahrscheinlichkeit

Gemäß ISO 26262 [ISO26262] ergibt sich die Schadenseintrittswahrscheinlichkeit (engl. Frequency of occurence of a hazardous event) aus der Kombination der *Exposition*sdauer (engl. Probability of exposure) in einer bestimmten *Fahrsituation* und der Möglichkeit der *Gefahrenabwehr* (engl. Controllability).

Exposition

Exposition/Aufenthalt in einer Betriebssituation, welche bei gleichzeitigem Auftreten des betrachteten Fehlers zu einer Gefährdung führen kann. [ISO26262]

Fahrsituation

Situation, welche während der Lebensdauer eines Fahrzeuges auftreten kann. [ISO26262]

Gefahrenabwehr/Kontrollierbarkeit

Möglichkeit eine *Gefahr* oder einen Schaden durch rechtzeitige Reaktion der beteiligten Individuen *abzuwehren*. [ISO26262]

5.1.8 Identifikation von Fahrszenarien

Im Folgenden werden potenziell kritische *Fahrsituationen* mit unterschiedlichen *Fahrzeugzuständen* (engl. operating mode) kombiniert; hieraus lassen sich verschiedene *Fahrszenarien* ableiten.

Fahrsituation

Die *Fahrsituation* oder der Umgebungszustand wird als Verknüpfung der Umstände bzw. Randbedingungen (z.B. nasse Fahrbahn, Glatteis etc.), die das Fahrer- und Fahrzeugverhalten beeinflussen verstanden.

Fahrzeugzustand

Der *Fahrzeugzustand* beschreibt den in einer Fahrsituation vorherrschenden Zustand der verschiedenen Fahrzeugsysteme. Für die Gefährdungsidentifikation und Risikobewertung von Interesse ist insbesondere der resultierende Bewegungszustand des Fahrzeuges (z.B. Fahrzeug steht, Fahrzeug fährt langsam, Fahrzeug fährt schnell, Fahrzeug verzögert stark etc.), da dieser das Schadensausmaß wesentlich mitbestimmt.

Fahrszenario

Das *Fahrszenario* ergibt sich durch die Kombination des relevanten Fahrzeugzustandes und der vorherrschenden Fahrsituation bzw. den Umgebungsbedingungen.

5.1.9 Bestimmung des Automotive Safety Integrity Levels

Für die Bestimmung des *Automotive Safety Integrity Levels (ASIL)* wird die zu entwickelnde System-Funktion hinsichtlich ihrer möglichen *funktionalen Fehler* analysiert.

Automotive Safety Integrity Level (ASIL)

ISO 26262 [ISO26262] definiert vier Sicherheitsanforderungsstufen, so genannte *Automotive Safety Integrity Level* (ASIL), wobei A den niedrigsten und D den höchsten Level darstellt. Je höher die ASIL-Einstufung ist, desto höhere Anforderungen ergeben sich an den Entwicklungsprozess und die Systemarchitektur. [ISO26262]

Funktionaler Fehler

Ein *funktionaler Fehler* ist eine nicht normale Bedingung, die möglicherweise dazu führt, dass eine Systemeinheit ihre spezifizierte Funktion nicht mehr oder nur eingeschränkt erfüllen kann. [IEC61508]

5.1.10 Risikobewertung

Anschließend werden die den ASIL bestimmenden Parameter subjektiv (*Subjektivität*) abgeschätzt und der ASIL kann aus der im ISO 26262 dokumentierten *Risikomatrix* abgelesen werden.

Subjektivität vs. Objektivität

Emotionalität führt dazu, dass Individuen ihre Umgebung bzw. einen Sachverhalt subjektiv (auf sich selbst bezogen) wahrnehmen. In diesem Sinne wird *Subjektivität* (lat. „Unterworfenheit“), also das Gültigsein allein für ein Subjekt, in den Naturwissenschaften zumeist als Fehlerquelle angesehen und zu vermeiden versucht. [HS04]
Im Unterschied dazu ist *Objektivität* dadurch charakterisiert, dass ein Sachverhalt aus einer gewissen Distanz unabhängig vom involvierten Individuum beschrieben wird bzw. gegenüber sinnlichen Wahrnehmungen abgesichert. Die Betrachtungsweise lässt demnach keine subjektiven Einflüsse zu. [RHE06, HS04]

Risikomatrix

Mit Hilfe einer *Risikomatrix* kann bestimmt werden, wie hoch das Risiko eines bestimmten Schadensereignisses ist. Die Matrix wird gemäß ISO 26262 durch das Schadensausmaß (vgl. Abschnitt: 5.1.6), die Expositionsdauer (vgl. Abschnitt: 5.1.7) und die Möglichkeit der Gefahrenabwehr (vgl. Abschnitt: 5.1.7) aufgespannt.

5.1.11 Objektiverung subjektiver Einflüsse

Ziel dieser Arbeit ist es das Vorgehen nach ISO 26262 zu objektivieren. Diese Objektivierung basiert auf der *Simulation* und *Analyse* von *Modellen*, welche die Problemstellung mit dem *Beschreibungsmittel* stochastische *Petrinetze* abbilden.

Simulation

Simulation ist die Nachbildung von Verhaltensweisen von Betrachtungseinheiten (z.B. technischer Systeme), Einflussgrößen oder Prozessen zur Feststellung interessierender Merkmale. In einer Simulation wird angestrebt Bedingungen und Verhältnisse so nachzubilden, wie sie in der Wirklichkeit bestehen. [Ste94b]

Analyse

Die *Analyse* ist die systematische Untersuchung eines Gegenstandes oder Sachverhaltes. Hierbei wird das zu untersuchende Objekt in seine Bestandteile zerlegt, um dessen elementaren Zusammenhänge zu ermitteln. [HS04]

Beschreibungsmittel, Methoden und Werkzeuge

Beschreibungsmittel dienen per Definition der graphischen, textuellen oder notationellen Formulierung planmäßiger Vorgehensweisen, Aufgabenstellungen und Lösungen.
Methoden werden als auf einem Regelsystem basierende Vorgehensweise zur Erlangung von Erkenntnissen deklariert.
Komplettiert werden die Betriebsmittel zur Systementwicklung bzw. -Analyse

durch *Werkzeuge*, mit Hilfe derer die Lösung von Problemen realisiert werden kann. *Werkzeuge* verkörpern die technische Umsetzung von Methoden . [Sch99b] Unter Verwendung der Anfangsbuchstaben der Entwicklungsmedien Beschreibungsmittel, Methoden und Werkzeuge hat sich im Bereich der Automatisierungstechnik das Akronym *BMW-Prinzip* [Sch99b] manifestiert.

Petrinetz

Ein *Petrinetz* ist ein formales Beschreibungsmittel zur Modellierung von Systemen bzw. Transformationsprozessen. Aufgrund seiner mathematischen Basis können diese bipartiten gerichteten Graphen [Sch99b, Sch99a] sowohl zur Spezifikation, als auch zum Design und zur Analyse von Systemen bzw. Prozessen genutzt werden [ISO15909].

Modell

Ein *Modell* ist eine Abstraktion eines bestimmten Ausschnittes der realen Welt oder eines anderen Modells. Es beschreibt einen Aspekt dieses Ausschnitts präzise und abstrahiert dabei von anderen Aspekten, die zur Analyse nicht von Bedeutung sind. [SPP03]

5.1.12 Ableitung von Sicherheitsanforderungen

Die nach ISO 26262 bestimmten ASIL-Einstufungen stellen *(Sicherheits-)Anforderungen* an die Entwicklung des Systems, um das von der Funktion ausgehende Risiko unterhalb einem, durch ein *Risikoakzeptanzkriterium* gegebenes Grenzrisiko zu fixieren.

(Sicherheits-)Anforderungen

Eine *(Sicherheits-)Anforderung* ist ein (sicherheitsbezogenes) Erfordernis, das einmal festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist. [ISO9000]

Risikoakzeptanzkriterium

Den Ausgangspunkt aller Risikobetrachtungen bilden nach [Bra06] so genannte *Risikoakzeptanzkriterien* (z.B. ALARP, GAMAB, MEM etc.), welche das tolerierbare Grenzrisiko (Restrisiko) festlegen, das bei Einhaltung der anerkannten Regeln der Technik von der Gesellschaft akzeptiert wird.

5.2 Begriffsgebäude

Immer wieder wird branchenunabhängig das Nicht-Vorhandensein von einheitlichen akzeptierten Begriffsystemen kritisiert [SSP10, SSS10]. So zeigt auch [Bör06] für die Entwicklung von sicheren Systemen auf, dass es aktuell noch kein einheitliches Gerüst der Begriffe und Definitionen gibt, sondern vielmehr in den verschiedenen Normen (IEC 61508, DIN EN 14971, DIN 40041, DIN 9000, VDI 31000) aus artverwandten Themenbereichen von unterschiedlichsten Definitionen und Begriffsbestimmungen ausgegangen wird.
Ziel dieses Abschnittes ist es, aufgrund der Abwesenheit des angesprochenen generischen anerkannten *Sicherheitsbegriffsgebäudes* ein zumindest für diese Arbeit geltendes Begriffsgerüst (s. Abb. 5.1) darzustellen, welches die wesentlichen im vorherigen Abschnitt definierten Begriffe in Relation setzt.
Zum besseren Verständnis wird das Begriffsystem jeweils durch natürlich-sprachliche Benennungen der gerichteten Relationen erweitert. Die Lesart der im Begriffssystem in Relation gesetzten Begriffe ist wie folgt: „Begriffs-Quelle“ → „Relations-Benennung“ → „Begriffs-Senke“ (z.B. „System“ → „ist“ → „Sachgut“; „IEC 61508“ → „ist Grundnorm von“ → „ISO 26262“ etc.).
Dieses Begriffsgebäude ist an verschiedenen Stellen um Hilfs-Begriffe bzw. „Anknüpf-Begriffe“ ergänzt, welche zwar nicht im vorherigen Abschnitt (s. Abschnitt 5.1) enthalten sind, dem Leser jedoch helfen das Begriffssystem in seinem Sprachgebrauch wiederzufinden (z.B. Sachgut, Umwelt etc.). Andere Hilfs-Begriffe werden eingefügt, um indirekte Relationen zwischen interessierenden Begriffen darzustellen (z.B. Schaden, Grenzrisiko etc.).
Die grau hinterlegten Begriffe bilden die Basis für das Verständnis des ASIL, weswegen deren Relationen in Abschnitt 6 weiter formalisiert und analysiert werden.

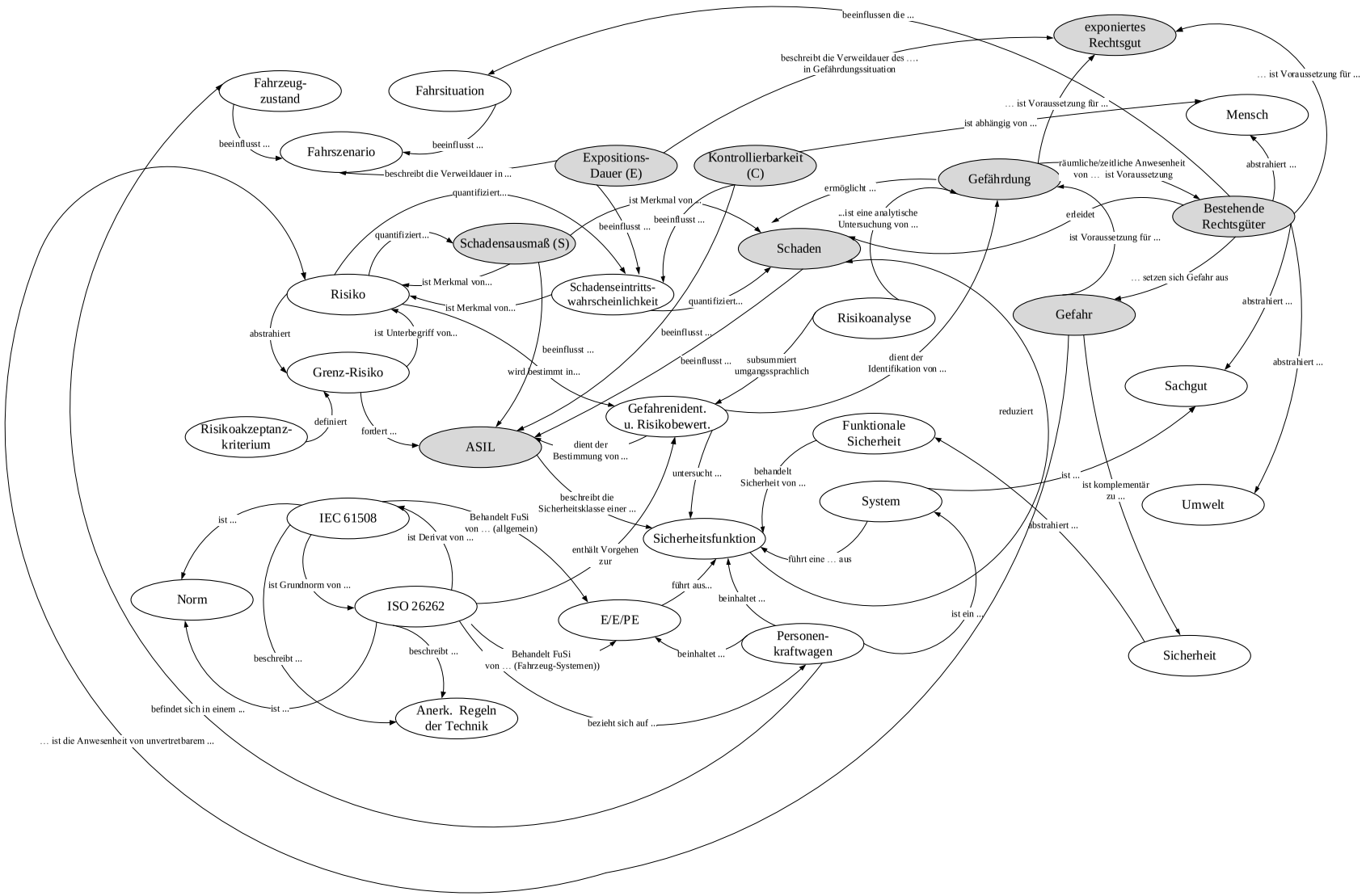


Abbildung 5.1: Begriffssystem – Funktionale Sicherheit im Kraftfahrzeugsektor

5.3 Zusammenfassung – Begriffsverständnis

In Kapitel 5 wird zur Bereitstellung der für diese Arbeit relevanten Fachtermini gezielt ein etwas anderer Ansatz gewählt, als es in vielen wissenschaftlichen Arbeiten, aber auch Standards der Fall ist. Hierbei wird von der bloßen Repräsentation einer strikt alphabetisch gereihten Liste von Begriffen und ihren begrifflich-sachlichen Erklärungen Abstand genommen und zu einer systematischen Gliederung entlang einer fachspezifischen „Storyline“ übergegangen.
Dies möglicherweise auf Kosten einer schnelleren Wiederfindbarkeit, aber dafür, basierend auf den jeweils verbal beschriebenen Relationen zu anderen Begriffen, zu Gunsten eines besseren und eindeutigen Verständnisses der Einzel-Begrifflichkeiten im fachspezifischen Kontext.
Aktuelle Ansätze des Terminologiemanagments [Bod06, Bud06, Stu07] gehen diesbezüglich einen noch weiter ausgreiften Weg, indem von einer rein verbalen Beschreibung der Relationen Abstand genommen wird, und die Begriffsrelationen werkzeuggestützt abgebildet (vgl. IGLOS [Sch09]) werden, um die Kommunikations-Effizienz noch weiter zu steigern.

Kapitel 6

Begriffliche Einordnung und Analyse des ASIL

In Kapitel 5 ist die auf Mehrdeutigkeit, Widersprüchlichkeit, Vagheit und Domänenspezifizität basierende Kommunikationsproblematik beschrieben, der im Rahmen dieser Arbeit mittels des in Abschnitt 5.1 dargestellten automobilspezifischen Definitionskataloges begegnet wird.
Diese rein definitorische Beschreibung reicht jedoch nicht aus, um den ASIL und seine Faktoren in dem Maße verstehen zu können, dass deren Wirkweise geeignet modelliert werden kann.
Hierzu bedarf es vielmehr einer fundierten begrifflichen Einordnung (s. Abschnitt 6.1) und Analyse (s. Abschnitt 6.2) des ASIL und seiner charakteristischen Faktoren.
Zweck dieses Vorgehens ist es zum einen, den in Kapitel 5 aufgezeigten Ursachen für eine fehlerbehaftete Kommunikation entgegenzuwirken. Von noch größerem Interesse ist die Analyse des Begriffsumfangs aber im Hinblick auf das Verständnis der später hinsichtlich ihrer Objektivierbarkeit zu diskutierenden (s. Abschnitt 8.1), den ASIL bestimmenden, Faktoren S, C und E.

6.1 Begriffliche Einordnung des ASIL in ein automotives Begriffsgebäude zur Funktionalen Sicherheit

Die Abbildungen 6.1 und 6.3 dienen der Visualisierung des die wesentlichen, den ASIL beeinflussenden, Begrifflichkeiten enthaltenden Begriffsgebäudes zur funktionalen Sicherheit in der Automobilindustrie. Im Rahmen der Modellierung dieses Begriffsgebäudes wird explizit der Anforderung nachgekommen die ASIL-Bestimmung unabhängig von der technischen Realisierung durchzuführen (vgl. 7.2 („General“) in ISO 26262). Hierbei soll lediglich die Funktion in kritischen Szenarien bewertet werden, weswegen auf eine mögliche detailliertere Modellierung des bestehenden Rechtsgutes *Ego-Fahrzeug* mit seinen Komponenten und deren Ausfallverhalten verzichtet wird.
Das Begriffsgebäude basiert einerseits auf der Beschreibung der prozessualen Begriffsrelationen (s. Abbildung 6.1) und andererseits auf der Abbildung der statischen Zusammenhänge zwischen existierenden potenziell exponierten bestehenden Rechtsgütern (s. Abb. 6.3). Hierbei kommen mit dem Beschreibungsmittel Petrinetz zur Modellierung der prozessualen Relationen und dem Beschreibungsmittel Klassendiagramm der UML zur Modellierung der statischen Zusammenhänge komplementäre Beschreibungsmittel zum Einsatz.

6.1.1 Prozessuale Begriffsrelationen

In [SS09] wird ein Ansatz aufgezeigt, ein dem DIN-Fachbericht 144 [DIN FB 144] konformes generisches Wirkmodell für einen Schadensablauf zu entwickeln. Abbildung 6.1 verwendet dieses Wirkmodell, adaptiert es auf die funktionale Sicherheit in der Automobilindustrie und erweitert es um die in der Sicherheitstechnik angewendeten Sicherungsimplementierungskonzepte. Des Weiteren differenziert es etwas stringenter zwischen den in der Sicherheitstechnik definierten Begriffen *Gefahr* und *Gefährdung* (vgl. auch Abschnitt 5.1.5).

Im Einzelnen setzt sich das Wirkmodell aus folgenden Begriffen zusammen.

- Im (angenommenen) Initialzustand *(P1 und P2 sind markiert)* des Modells

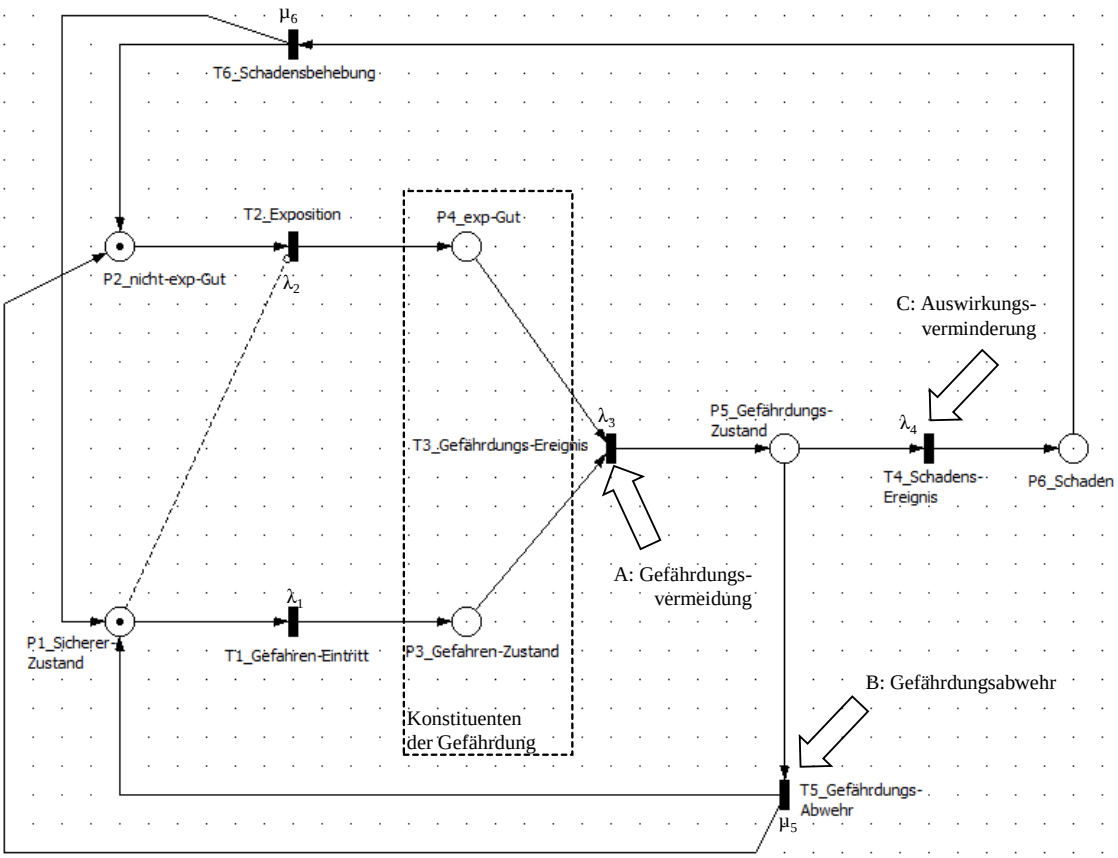


Abbildung 6.1: Begriffsgebäude der funktionalen Sicherheit im Automobilbereich

befindet sich ein wie auch geartetes Rechtsgut (vgl. Abschnitt 6.1.2) in einem *sicheren Zustand*. Das Rechtsgut ist keiner Gefährdung ausgesetzt, es ist nicht exponiert (z.B. Ego-Fahrzeug fährt auf Autobahn).

- Im Folgenden entwickelt sich eine *gefährliche Situation* (=Gefahreneintritt) *(λ_1 schaltet)* und es resultiert eine *Gefahr* bzw. ein *Gefahrenzustand (P2 und P3 sind markiert)*. Das Rechtsgut ist nach wie vor nicht exponiert, d.h. die Entwicklungsmöglichkeit zu einer Gefährdung wird aktuell noch nicht ausgeschöpft (z.B. einen Kilometer vor dem Ego-Fahrzeug verliert ein vorherfahrendes Fahrzeug Öl und es bildet sich eine Ölspur).

- Anschließend nähert sich ein Rechtsgut der vorherrschenden Gefahr an, bis deren zeitliches und räumliches Aufeinandertreffen letztendlich nicht mehr abwendbar ist (z.B. das Ego-Fahrzeug befindet sich unmittelbar vor der Ölspur, ein Ausweichen ist nicht mehr möglich).

- Im nächsten Schritt kommt es zu einem *Gefährdungs-Ereignis (λ_3 schaltet)*. Aus dem Gefährdungsereignis resultiert die *Gefährdung* bzw. der *Gefährdungszustand*.

- Die *Gefährdung (P5 ist markiert)* bzw. der Gefährdungszustand ist ein Zustand mit Schadenspotenzial (z.B. Ego-Fahrzeug überfährt Öl-Spur). Er kann sich potenziell zu einem *Schaden* auswirken.

- Gemeinsam mit den *bestehenden Rechtsgütern (P4 ist markiert)* (Mensch, Güter, Umwelt) konstituiert der Gefahrenzustand die *Gefährdung(-ssituation)*. In einer Gefährdungssituation sind Menschen, Güter und/oder Umwelt einer oder mehrerer Gefährdungen ausgesetzt (Exposition). Nur wenn eine Gefährdungssituation als Koinzidenz von Gefährdung und Rechtsgütern vorliegt, kann ein *Schadensereignis (λ_4 schaltet)* eintreten und der *Gefährdungszustand* zu einem *Schaden (P6 ist markiert)* führen (z.B. Verunfallung Ego-Fahrzeug aufgrund Kontrollverlust durch Ölspur).

- Im Hinblick auf das weitere Modellverhalten stellt der Gefährdungszustand eine wahrscheinlichkeitsbehaftete Entscheidung dar, da der weitere Prozessverlauf in hohem Maße vom Zustand der *bestehenden Rechtsgüter* und deren aktueller Konstellation abhängig ist. So kommt dem Rechtsgut *Person* (vgl.

Abb. 6.3) im Sinne der Risikoanalyse nach ISO 26262 die Rolle des Operators, d.h. des das Fahrszenario beeinflussenden Individuums (z.B. Fahrzeugführer, Fußgänger etc.) zu Teil, welcher je nach Gefährdungssituation:

  - die Möglichkeit hat kontrollierend einzugreifen *(μ_5 schaltet)* und in einen „sicheren Zustand“ *(P1 und P2 sind markiert)* zu gelangen (z.B. der Fahrer behält durch einen Regeleingriff die Kontrolle über das Ego-Fahrzeug)
  - keine Möglichkeit hat die Gefährdungssituation zu kontrollieren und damit das Schadensereignis nicht mehr verhindern kann

- Der Begriff des *Schadens* als Resultat der Kausalkette umfasst ganz allgemein die Minderung bestehender Rechtsgüter [SS09].

- Ist ein Schaden eingetreten, kann das System, bestehend aus Fahrzeug, Umgebung etc. nur noch über Maßnahmen der *Schadensbehebung (μ_6 schaltet)* wieder in den *sicheren Zustand* überführt werden (z.B. Abschleppen und Instandsetzung des Fahrzeuges).

Des Weiteren sind im Wirkmodell zur Erreichung eines besseren Gesamtverständnisses die wesentlichen Sicherungsimplementierungskonzepte der Sicherheitstechnik nach [Dre09] und [Bör06] auf die Automobilindustrie projiziert.
Diese sind:

- **Gefährdungsvermeidung:** Vermeidung des Übergangs von einem sicheren in einen globalen Gefährdungszustand (s. Abbildung 6.1: A).

- **Gefährdungsabwehr:** Der Übergang in den Gefährdungszustand wird zugelassen; mit geeigneten Mitteln wird versucht wieder in den sicheren Zustand zu gelangen (s. Abbildung 6.1: B).

- **Auswirkungsverminderung:** Man geht vom Eintreten eines Schadenszustandes aus und konzentriert sich darauf das Schadensausmaß durch geeignete Maßnahmen zu reduzieren (s. Abbildung 6.1: C).

Hieraus wird deutlich, dass die Sicherungsimplementierungskonzepte Gefährdungsvermeidung (z.B. durch inhärent sichere Konstruktion), Gefährdungsabwehr und Auswirkungsminderung (jeweils durch technische Schutzmaßnahmen) erst dann geeignet spezifiziert werden können, wenn die zu verhindernde Gefährdung und die

ihnen zugrunde liegenden Ursachen identifziert und hinsichtlich ihrer Eintrittswahrscheinlichkeit analysiert wurden.
Insbesondere auf der Ebene der Gefährdungsvermeidung, welche gemäß nachstehender Anforderung aus der ISO 26262 im Mittelpunkt der ASIL-Einstufung steht, erfordert dies eine umfangreiche Analyse der Fahrzeug- und Umgebungszustände, so wie deren Zustandsabhängigkeiten (z.B. keine 200 km/h in der Innenstadt), um die Eintrittswahrscheinlichkeit von gefährlichen Konstellationen lokaler Zustände ermitteln zu können.

> The objective of the hazard analysis and risk assessment is to identify and categorise the hazards of the item and formulate the safety goals related to the *prevention or mitigation of these hazards*, in order to avoid unreasonable risk. (Anforderung 7.1 aus ISO 26262)

Dies liegt u.a. darin begründet, dass für die Eintrittswahrscheinlichkeiten bestimmter Gefährdungssituationen häufig keine gesicherte Datenbasis zur Verfügung steht, weswegen diese aus den Einzelwahrscheinlichkeiten der auslösenden Gefährdungsereignisse (inkl. Umgebungseinflüsse) zu ermitteln ist.
Um ein für spätere Betrachungen erforderliches detaillierteres Verständnis der den ASIL beeinflussenden Faktoren zu erlangen, wird das Begriffs-Modell abschließend einer formalen Analyse unterzogen. Hierzu wird der Erreichbarkeitsgraph (s. Abbildung 6.2) des die prozessualen Zusammenhänge abbildenden Petrinetz-Modells erstellt. Dabei wird von der oben beschriebenen und in Abbildung 6.1 dargestellten Anfangsmarkierung ausgegangen.

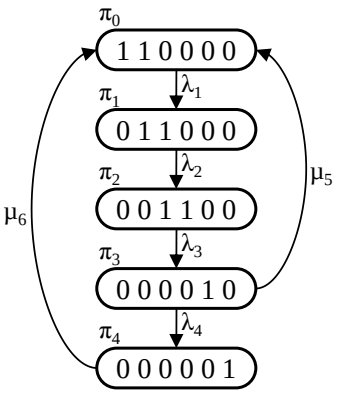


Abbildung 6.2: Erreichbarkeitsgraph Begriffsmodell

Aus dem Erreichbarkeitsgraph (s. Abbildung 6.2) lässt sich folgende Zustandsübergangsmatrix Q bestimmen:

$$Q = \begin{pmatrix} -\lambda_1 & 0 & 0 & \mu_5 & \mu_6 \\ \lambda_1 & -\lambda_2 & 0 & 0 & 0 \\ 0 & \lambda_2 & -\lambda_3 & 0 & 0 \\ 0 & 0 & \lambda_3 & -\lambda_4 - \mu_5 & 0 \\ 0 & 0 & 0 & \lambda_4 & -\mu_6 \end{pmatrix}$$

Mit der Randbedingung $Q\pi = 0$ ergibt sich für den Zustand $P_{5-Gefaehrdungszustand}$ $(= \pi_3)$, die Wahrscheinlichkeit dieses Zustandes ist im Zuge der Abschätzung der Expositionswahrscheinlichkeit in einem bestimmten Szenario von Interesse, nachfolgende Gleichung:

$$\pi_3 = \frac{\lambda_3}{\lambda_4 + \mu_5}\pi_2 \tag{6.1}$$

Mittels dieser Analyse des Begriffsgebäudes kann formal nachgewiesen werden, dass die Expositionswahrscheinlichkeit in der Realität von den Einflussfaktoren λ_3 (=bedingte[1] Rate des Gefährdungsereignisses), λ_4 (=Rate der „Nicht-Gefährdungsabwehr“ bzw. des Schadensereignisses) und μ_5 (=Rate der Gefährdungsabwehr) abhängig ist. Diese Abhängigkeit wird von der ISO 26262 durch die Forderung einer unabhängigen Schätzung des Faktors E ignoriert, wodurch die Aussagekraft der geschätzten Expositionswahrscheinlichkeit in Frage gestellt werden kann.
Im Zuge der in späteren Abschnitten beschriebenen Untersuchungen wird diese Abhängigkeit jedoch vernachlässigt, um die EmMORI-Methode konform den in ISO 26262 gestellten Anforderungen anwenden zu können.
Über die den ASIL mitbestimmenden Parameter C und S können durch die formale Analyse des entwickelten Petrinetz-Modells keine weiteren Erkenntnisse gewonnen werden. Dies liegt darin begründet, dass das Modell lediglich Aussagen über das Häufigkeitsgerüst von auftretenden Situationen bzw. Szenarien zulässt. Das aus den Situationen bzw. Szenarien resultierende Schadensausmaß oder die, die Kontrollierbarkeit im jeweiligen Szenario beeinflussenden physiologischen und psychologischen Faktoren, sind im Modell nicht abgebildet.

[1] bedingt, da π_2 vorausgesetzt

6.1.2 Statische Begriffsrelationen

Die zweite Säule des entwickelten Begriffsgebäudes zur automobilen funktionalen Sicherheit wird durch die statische Abbildung (s. Abb. 6.3) der Rechtsgüter (P_2 und P_3 aus Abbildung 6.1) aufgespannt, welche potenziell einem Gefährdungs-Zustand (P_5) ausgesetzt werden können und so eine Gefährdungsituation konstituieren.
Die Rechtsgüter können hierbei in Anlehnung an [Sch09] wie in Abbildung 6.3 dargestellt in Gegenstände bzw. Objekte, Natur bzw. Umwelt und Personen unterschieden werden.

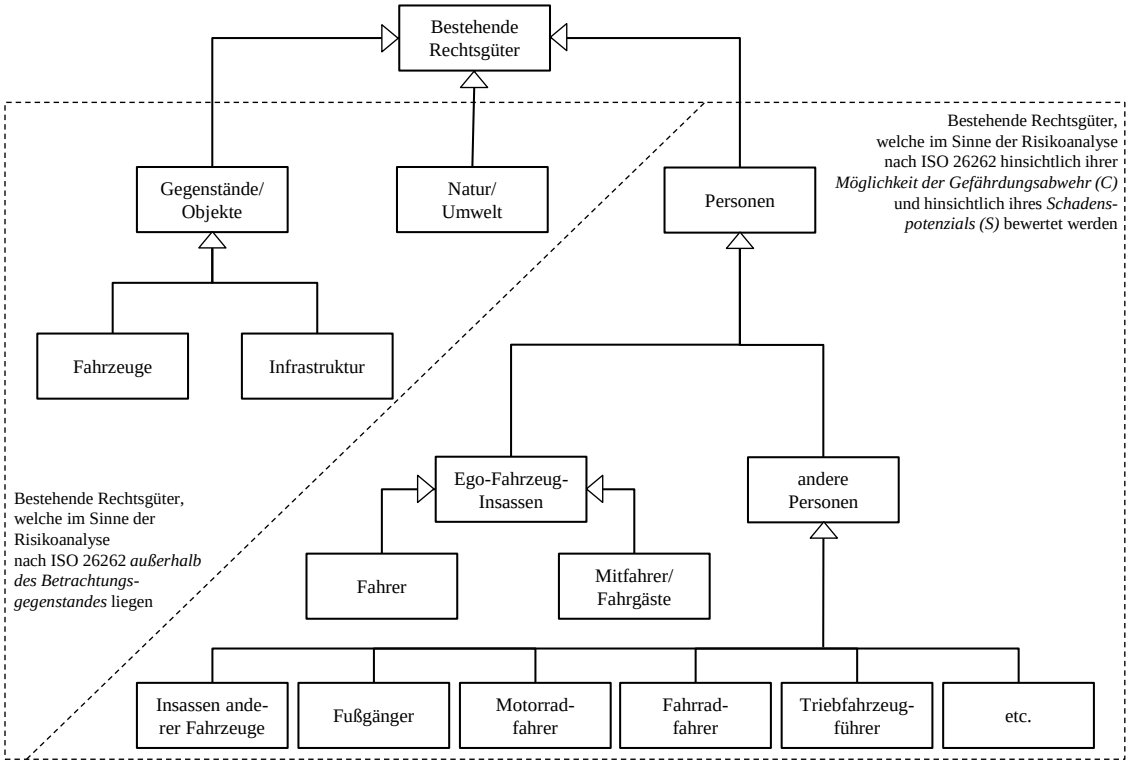


Abbildung 6.3: Begriffsgebäude der bestehenden Rechtsgüter (anglehnt an [Sch09])

Für die Risikoanalyse nach ISO 26262 sind lediglich die Personen von Interesse. Diese können mit einer gewissen Wahrscheinlichkeit einen Gefährdungs-Zustand kontrollieren (T_5) und ein Schadensereigniss abwenden. Gelingt es dem Rechtsgut Mensch nicht den Zustand zu kontrollieren, resultiert ein Schadensereignis, welches mit einem Schaden, also einer Minderung der bestehenden Rechtsgüter, einhergeht. Diese Minderung kann, wie nachstehende Beispiele zeigen, jede der drei genannten

Rechtsgut-Kategorien betreffen.

- Kollision des Ego-Fahrzeuges mit Infrastruktur-Elementen → Schädigung an *Objekt*
- Auslaufen von Benzin nach Verunfallung des Ego-Fahrzeuges → Schädigung *Natur*
- Kollision mit Fußgänger → Schädigung bzw. Verletzung *Person*

Im Zuge der Risikoanalyse nach ISO 26262 werden nur Personen-Schäden bewertet. Die Gruppe der potenziell exponierten Personen kann theoretisch beliebig feingranular differenziert betrachtet werden. Im Rahmen des hier vorgestellten Modells wird das generische Rechtsgut *Person* lediglich noch in *Ego-Fahrzeug-Insassen* und ihre potenziellen menschlichen Ausprägungen Fahrer und Mitfahrer, und *andere Personen* wie Insassen anderer Fahrzeuge oder Fußgänger, untergliedert.
Ist eine Gefährdungssituation existent haben die verschiedenen am Verkehr beteiligten Personen sehr unterschiedliche, von diversen Faktoren abhängige (vgl. Abschnitt 8.1.3), Möglichkeiten ein Schadensereignis abzuwenden.
Können sie die Gefährdungs-Situation nicht beherrschen, kommt es zu einem Schaden, dessen Ausmaß wiederum in hohem Maße von den unterschiedlichen am Schadensereignis beteiligten Personen abhängig ist (vgl. Abschnitt 8.1.1).

6.2 Begriffliche Analyse des ASIL

Der terminologische Vergleich des allgemeinen Risikobegriffes, wie er in Anlehnung an ISO/IEC 51 in IEC 61508 hinterlegt ist, mit dem im ISO 26262 auf den ASIL projizierten Risikobegriff lässt sich wie in Abbildung 6.4 dargestellt visualisieren.

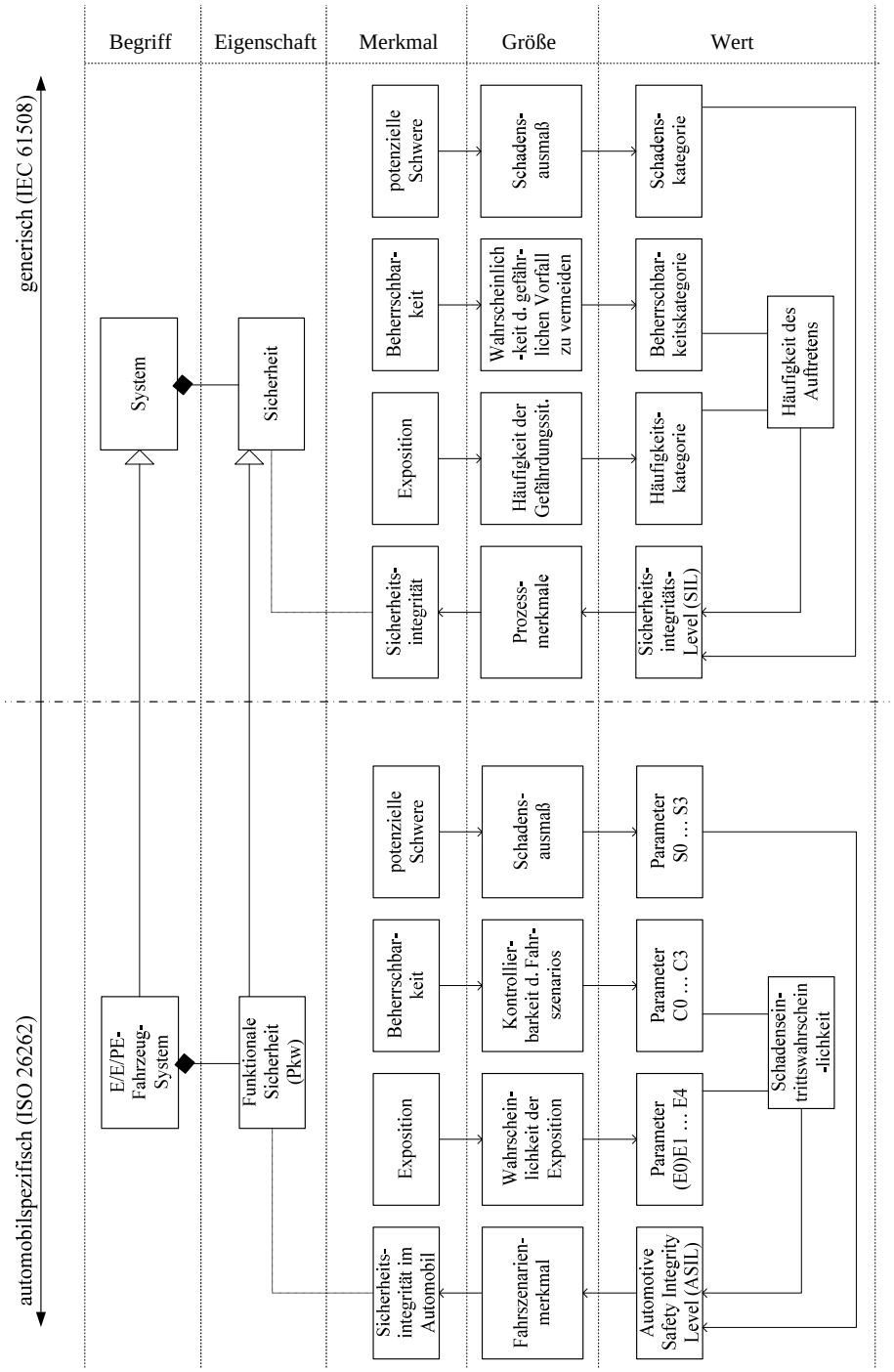


Abbildung 6.4: Allgemeines und konkretes Begriffsgebäude der Sicherheitsintegrität (basierend auf [Sch09])

Der „Automotive Safety Integrity Level“ ist nach ISO 26262 als einer von fünf Leveln (QM, ASIL A, B, C und D) definiert, mittels welchem einem System Anforderungen nach ISO 26262 und Sicherheitsmaßnahmen zur Abwendung von unzumutbaren bzw. unvertretbaren Restrisiken zugewiesen werden (vgl. Abbschnitt 5.1.9).
Die inhaltliche formale Basis des Risikomaßes „Automotive Safety Integrity Level“ wird durch den Begriff des „(Rest-)Risiko“ aufgespannt.
Um den Risikobegriff selbst hinreichend zu verstehen, ist es hilfreich, die ihn charakterisierenden Begriffskonstituenten zu diskutieren. Anschließend kann das Risiko formal auf den ASIL abgebildet werden, um Analogien nachzuweisen bzw. aufzuzeigen.
Gemäß ISO/IEC Guide 51 [ISO51] – hierbei handelt es sich um einen Leitfaden, zur Einbindung von Sicherheitsaspekten in Standards und Normen jeglicher Branchen – lässt sich das Begriffsgebäude um den Risikobegriff wie in Abbildung 6.5 dargestellt definieren.

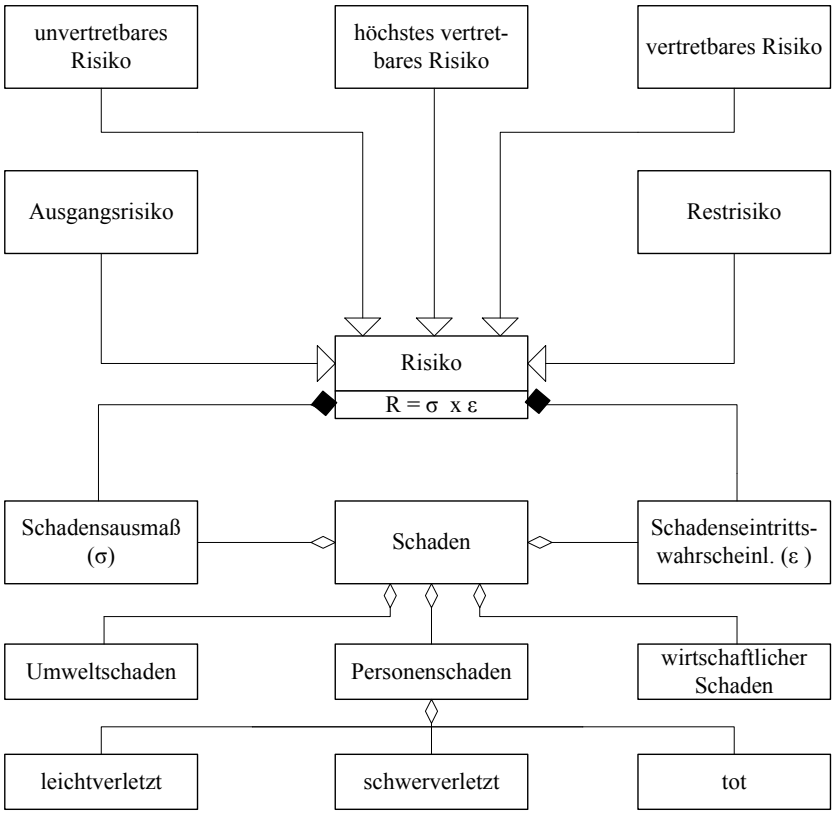


Abbildung 6.5: Risiko-Begriffsgebäude [Sch09]

Abbildung 6.5 zeigt ein an die UML angelehntes Klassendiagramm, welches die wesentlichen den Risikobegriff ausmachenden Begriffe visualisiert. Um das *Risiko* zu erklären, bedarf es insbesondere des Begriffs des *Schadens* [SSS09]. Schäden, welche in Bezug auf das beeinträchtigte Rechtsgut (Person, Umwelt, wirtschaftlicher Schaden) unterschieden werden können, sind hierbei Zufallsvariablen, denen eine Verteilung hinterlegt werden kann. Das zugehörige Risiko (R) lässt sich nach [IEC61508] durch die Kombination des *Ausmaß* des Schadens (σ) und der *Eintrittswahrscheinlichkeit* des Schadens (ϵ) bestimmen.
Dieser Zusammenhang lässt sich durch folgende, allgemein akzeptierte Risikoformel (vgl. [Bae08]) definieren:

$$R = \sigma * \epsilon \tag{6.2}$$

ISO 26262 greift die Konstituenten dieser Risikoformel zur Bestimmung des ASIL auf und erweitert sie um den Aspekt der Kontrollierbarkeit (C) der gefährlichen Situation durch exponierte Personen (z.B. Fahrer, Fußgänger etc.)
Dem Risikomerkmal „Schadensausmaß“ (σ) wird in ISO 26262 das direkte Analogon „Severity“ (S) zugewiesen. Das Ausmaß eines aus der Dysfunktion der zu entwickelnden Funktion resultierenden Schadens wird abgeschätzt, indem potenzielle aus einem Schadensereignis resultierende Konsequenzen einer von vier ordinalen Schwerekategorien (s. Tabelle 6.1) zugeordnet werden.

Tabelle 6.1: Merkmale des Automotive Safety Integrity Levels

Parameter	Description	Classes			
		very low probability..... high probability no injuries .....fatal injuries uncontrollable ..... controllable in general			
E	Probability of exposure	E1	E2	E3	E4
S	Severity	S0	S1	S2	S3
C	Controllability	C3	C2	C1	C0

Die „Schadenseintrittswahrscheinlichkeit“ nach IEC 61508 wird gemäß ISO 26262 als eine Kombination zweier Wahrscheinlichkeiten interpretiert, welche unabhängig voneinander geschätzt werden. Hierbei handelt es sich auf der einen Seite um die

Wahrscheinlichkeit, dass sich ein Fahrzeug überhaupt in einer gefährlichen Fahrsituation befindet (Probability of exposure in the operational situation (E)), und auf der anderen Seite um die Wahrscheinlichkeit, dass der Fahrer oder andere Verkehrsteilnehmer in der Lage sind das gefährliche Ereignis abzuwenden und den Schaden eines bestimmten Ausmaßes vermeiden können (Controllability (C)). Beiden Wahrscheinlichkeitsgrößen wird gemäß ISO 26262 einer von vier ordinalen Wahrscheinlichkeits-Werten zugeordnet (s. Tabelle 6.1)[2].
Basierend auf diesen Parametern wird einer zu entwickelnden Funktion eine von fünf (Sicherheits-)Anforderungsstufen – Automotive Safety Integrity Leveln (ASIL 1-4 & QM) – zugewiesen. Hierzu wird die Summe der Elemente der einzelnen Parameter der drei ASIL-Konstituenten Expositionswahrscheinlichkeit $E = \{1, 2, 3, 4\}$, Schadensausmaß $S = \{0, 1, 2, 3\}$ und Kontrollierbarkeit $C = \{0, 1, 2, 3\}$ (vgl. Tabelle 6.1) gebildet und gemäß nachstehenden Rechenvorschriften der ASIL aus der Menge $ASIL = \{QM, A, B, C, D\}$ bestimmt (vgl. Tabelle 7.1).

$$E_i + S_i + C_i < 7 \rightarrow QM \tag{6.3}$$

$$E_i + S_i + C_i = 7 \rightarrow ASIL\ A \tag{6.4}$$

$$E_i + S_i + C_i = 8 \rightarrow ASIL\ B \tag{6.5}$$

$$E_i + S_i + C_i = 9 \rightarrow ASIL\ C \tag{6.6}$$

$$E_i + S_i + C_i = 10 \rightarrow ASIL\ D \tag{6.7}$$

Mit steigendem ASIL steigen auch die Anforderungen an die Sicherheit, die in den verschiedenen Teilen der Norm spezifiziert sind. An Funktionen deren Kritikalität der (Sicherheits-)Anforderungsstufe QM zugeordnet wird, werden keine Anforderungen gestellt, die über das übliche Qualitätsmanagement hinausgehen.
Im folgenden soll der Zusammenhang (vgl. Abbildung 6.6) zwischen der allgemeinen kontinuierlichen Risikoformel $R = \sigma * \epsilon$ und dem ordinalen semi-quantitativen Risikomaß ASIL ($ASIL = E + S + C$) analysiert werden, dessen Konstituenten gleichermaßen ordinal skaliert sind.

[2]Diese Zusammenhänge zwischen den generischen und den automobilspezifischen Risikomerkmalen werden in dem die Risikoanalyse-Ansätze nach IEC 61508 und ISO 26262 vergleichenden Abschnitt 7.2.3 noch einmal im Detail aufgegriffen (vgl. Tabelle 7.5).

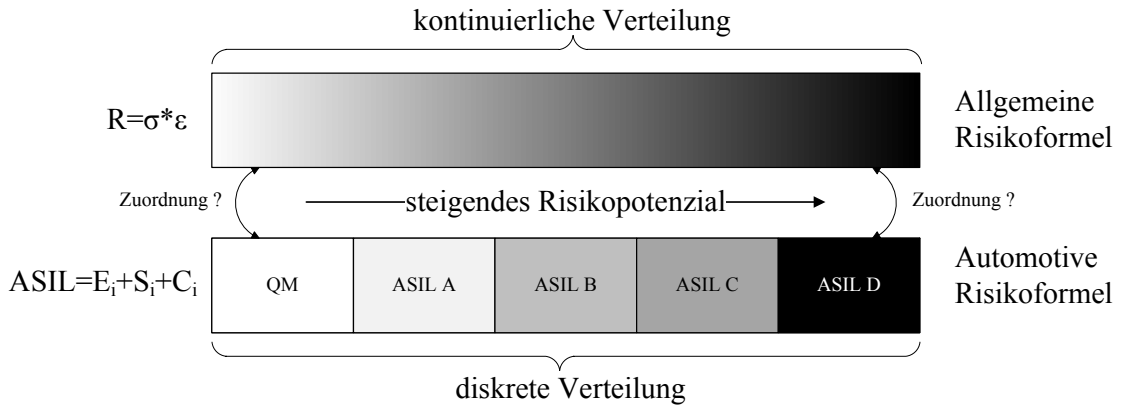


Abbildung 6.6: Die allgemeine und die automotive „Risikoformel“

Die Summanden sind für E und S aufsteigend und für C absteigend über 4 bzw. 5 Stufen ordinal skaliert (vgl. Tab. 6.1).
Die umgekehrte Skalierung des Parameters C erscheint zunächst im Vergleich zu den anderen beiden Parametern inkonsistent. Die Konsistenz bleibt aber gewahrt, wenn man bedenkt, dass mit dem Faktor C zunächst die Kontrollierbarkeit eines gefährlichen Szenarios, und nicht dessen Nicht-Kontrollierbarkeit bewertet wird. Nimmt man die umgekehrte Folge zur Definition einer Nicht-Kontrollierbarkeit $\overline{C} = 1 - C$, so besteht hier eine Analogie zur Wahrscheinlichkeit der Beibehaltung einer vorherrschenden Gefährdung.
Unter dieser Annahme ergibt sich die ursprüngliche Formel zur Berechnung des ASIL zu:

$$ASIL = S + E + (1 - C) \tag{6.8}$$

Um die allgemeine, ein kontinuierliches Verhalten beschreibende, Risikoformel $R = \sigma * \epsilon$ auf diese Gleichung zur ASIL-Bestimmung abbilden zu können, wird diese logarithmiert. Nach Logarithmierung ergibt sich die Summe:

$$\log R = \log \sigma + \log \epsilon \tag{6.9}$$

Auf Basis der Gleichungen 6.8 und 6.9 kann das Schadensausmaß (S) nach ISO 26262 dem Logarithmus des generischen Schadensausmaßes ($\log \sigma$) zugeordnet werden.

$$\log \sigma \rightarrow S \tag{6.10}$$

Analog kann der Wahrscheinlichkeit der Beibehaltung einer vorherrschenden Gefährdung $(E + (1 - C))$ gemäß ISO 26262 der Logarithmus der Schadenseintrittswahrscheinlichkeit $(\log \epsilon)$ zugeordnet werden.

$$\log \epsilon \rightarrow E + (1 - C) \tag{6.11}$$

Im Folgenden wird die Relation zwischen dieser formalen Herleitung und dem in Abschnitt 6.1.1 beschriebenen prozessualen Begriffsgebäude (vgl. Abb. 6.1) diskutiert. Abbildung 6.1 verdeutlicht, dass die für die Bestimmung des ASIL interessierende Aufenthaltswahrscheinlichkeit (Exposure) in einem gefährlichen Fahrszenario nachfolgendem Funktionszusammenhang gehorcht:

$$P_{5\_Gefaehrdungs-Zustand} = +f(\lambda_3) - f(\lambda_4) - f(\mu_5) \tag{6.12}$$

Die Aufenthaltswahrscheinlichkeit in einem gefährlichen Szenario (P_5) erhöht sich also mit wachsender Gefährdungs-Eintrittsrate (λ_3) und wird sowohl durch die Wahrscheinlichkeit des Eintritts eines Schadens (λ_4), als auch durch die Wahrscheinlichkeit der Kontrollierbarkeit (μ_5) des gefährlichen Szenarios durch ein beteiligtes Individuum reduziert.
Eben dieser Zusammenhang spiegelt sich auch in Gleichung 6.11 wieder, welche die Relation zwischen der generischen Risiko-Konstituente ϵ und den automobilen Zuordnungen beschreibt. So wirkt sich eine Erhöhung der Expositionswahrscheinlichkeit (E) gleichermaßen erhöhend auf die generische Konstituente ϵ aus; eine Erhöhung der Kontrollierbarkeit (C) bewirkt dagegen die Reduktion von ϵ.
Hiermit können die in Abschnitt 6.1.1 modelltheoretisch hergeleiteten Zusammenhänge durch die formale Gegenüberstellung des automobilspezifischen ASIL mit dem generischen Risikobegriff nachgewiesen werden.

Kapitel 7

Sicherheitsplanung im Automobilwesen

In Abschnitt 1.2 wurde auf die Notwendigkeit der Durchführung einer strukturierten Sicherheitsplanung hingewiesen, um Sicherheitsaspekte von Beginn an in ein System zu integrieren. Um die Sicherheitsplanung zu stützen wird in ISO 26262 die Erstellung eines Sicherheitsplans gefordert.
Dieser Sicherheitsplan umfasst alle Tätigkeiten, die zum Erreichen der Funktionalen Sicherheit erforderlich sind. Hierunter fallen sowohl solch organisatorische Aspekte wie die *Zeitplanung* und *Zuweisung von Verantwortlichkeiten* im Projekt, als auch die Durchführung und Dokumentation einer *Risikoanalyse*, die Planung von *Verifikations- und Validationsaktivitäten* und eine *Zusammenstellung der Maßnahmen* zur Vermeidung bzw. Beherrschung von systematischen Fehlern.
Da die Risikoanalyse im Rahmen dieser Arbeit von übergeordnetem Interesse ist, wird in Abschnitt 7.1 zuerst ein kurzer Abriss über allgemeine, vom normativen Kontext losgelöste, Vor- und Nachteile der Durchführung von Risikoanalysen gegeben, bevor in Abschnitt 7.2 im Detail auf die in ISO 26262 und IEC 61508 vorgeschlagenen Vorgehensweisen zur Risikoanalyse eingegangen wird.

7.1 Risikoanalysen im Automobilsektor

Die Durchführung von Risikoanalysen ist aufwendig, teuer, und es dauert in der Regel relativ lange bis Sicherungsmaßnahmen identifziert, ausgewählt und realisiert werden [Ste94b].

Trotz allem sollte die Durchführung einer Risikoanalyse auch dann in Erwägung gezogen werden, wenn sie normativ nicht gefordert ist. Diese These liegt darin begründet, dass die Vorteile, welche sich aus der Durchführung einer Risikoanalyse ergeben, die negativen Aspekte deutlich überwiegen.
So fördert die Beschäftigung mit dem Thema Risikoanalyse sowohl das Verständnis von sicherheitsrelevanten Zusammenhängen als auch das Sicherheitsbewusstsein von Mitarbeitern, direkten Vorgesetzten und Entscheidungsträgern. Außerdem ist die Risikoanalyse ein adäquates Mittel um Schwachstellen im System aufzudecken und diesen mit angemessenen Sicherungsmaßnahmen entgegenzuwirken [Ste94b].
Des Weiteren besteht der Wert der Risikoanalyse auch im Zwang, Entscheidungen bewusst zu treffen, zu begründen und sie nachvollziehbar zu dokumentieren [OS04]
Um bei fehlendem normativen Zwang die Entscheidung für oder gegen die Durchführung einer Risikoanalyse zu erleichtern, werden in [Ste94b] eine Reihe von Kriterien bzw. Entscheidungshilfen gegeben. Stelzer postuliert, dass Risikoanalysen nur dann durchgeführt werden sollten, wenn mindestens eines der folgenden Kriterien erfüllt ist:

- Das zu entwickelnde Systeme ist komplex und mögliche Konsequenzen gefährdender Ereignisse sind nur schwer überschaubar.
- Es handelt sich um ein neuartiges und in seiner Sicherheitsrelevanz noch unbekanntes System.
- Die mit dem Betrieb des Systems verbundenen potenziellen Schäden sind sehr hoch.

Zudem sollten Risikoanalysen nur dann geplant und durchgeführt werden, wenn es Sachkundigen nicht ohne weitere Analysen möglich ist, angemessene Sicherungsmaßnahmen vorzuschlagen und ausreichende Mittel – monetär und personell – zur Verfügung stehen.

7.2 Risikoanalysen im normativen Kontext

Im Rahmen der Entwicklung von sicherheitsrelevanten E/E/PE-Systemen für Straßenfahrzeuge ist der Hersteller vom Gesetzgeber verpflichtet eine Risikoanalyse durchzuführen, um dem Stand der Technik zu genügen. Hierbei kann der Hersteller, wie

in Abschnitt 2.1 dargelegt, in der Praxis aktuell die Risikoanalyse nach ISO 26262-3 (produkthaftungsrechtlich nicht abgesichert) oder nach IEC 61508-1 anwenden.
Im Rahmen dieses Abschnitts wird das Hauptaugenmerk auf die in ISO 26262 vorgeschlagene Vorgehensweise (s. Abschnitt 7.2.1) gelegt, da diese in Zukunft immer wichtiger werden wird, und es das Ziel dieser Arbeit ist, diese Methode zu objektivieren.
Auf die in der Sicherheitsgrundnorm beschriebenen Ansätze wird nur punktuell eingegangen (s. Abschnitt 7.2.2), um die grundlegenden Unterschiede, aber auch Gemeinsamkeiten, aufzuzeigen.
Eine Möglichkeit den normativen Anforderungen zu genügen wird anhand der einfachen Beispielfunktion *Abblendlicht* dargestellt.

7.2.1 Risikoanalyse nach dem Automotive-Derivat ISO 26262

Im Zuge der normkonformen Entwicklung eines sicherheitsrelevanten E/E/PE-Fahrzeugsystems gilt es nach ISO 26262 zu bewerten, welcher Sicherheitsklasse (ASIL) dessen System-Funktion zuzuordnen ist, um die daraus resultierenden ASIL-abhängigen Anforderungen an den Entwicklungsprozess und/oder die Systemauslegung ableiten zu können.
Ziel der Gefährdungsanalyse und Risikobewertung ist es, das Risiko eines sicherheitskritischen Ereignisses auf ein vertretbares Maß, das akzeptierte Risiko (s. Abb. 7.1), zu reduzieren, um die Sicherheit der Verkehrsteilnehmer zu gewährleisten.
Um die Sicherheitsklasse einer Funktion zu bestimmen, werden in ISO 26262 nachstehende Schritte definiert, welche im Folgenden für die *Funktion Abblendlicht* aufgezeigt werden.

1. **Allgemeine System-/Funktionsbeschreibung**
   Darstellung des Zieles, welches mit dem zu realisierenden Systems bzw. der zu realisierenden Funktion erreicht werden soll.

> *Das Abblendlicht dient der Ausleuchtung der Fahrbahn vor dem Fahrzeug, sowie dazu von entgegenkommenden bzw. anderen Verkehrsteilnehmern gesehen zu werden.*

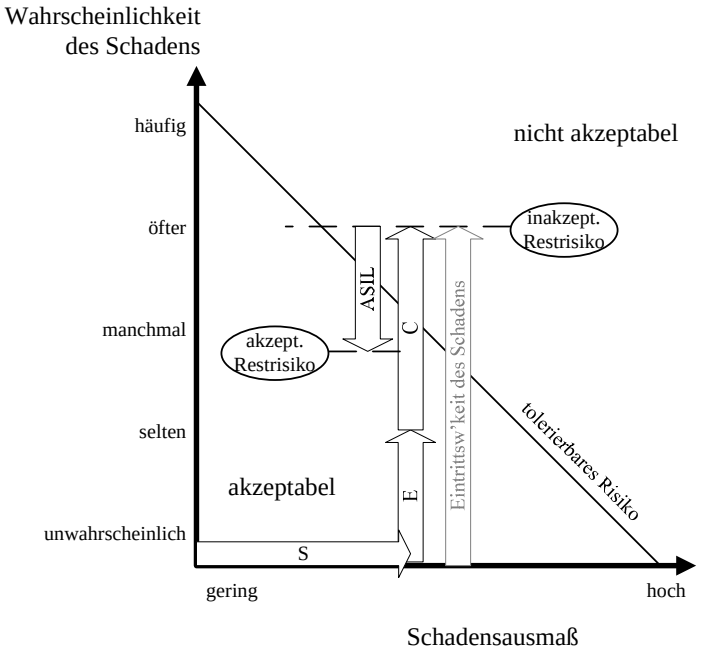


Abbildung 7.1: Visualisierung des ASIL [Rau08]

2. **Beschreibung der geforderten Funktionalität**
   Beschreibung der relevanten Sub-Funktionen, welche die Gesamtfunktionalität ausmachen.

> *Anforderung „Licht ein“ überführt das die Funktion realisierende System in den Zustand „Licht EIN“*
>
> *Anforderung „Licht aus“ überführt das die Funktion realisierende System in den Zustand „Licht AUS“*

3. **Beschreibung der möglichen Fahrsituationen**
   Fahrsituationen können mittels verschiedener Umgebungsmerkmale-/Kriterien (z.B. sichteinschränkende Merkmale, Straßentyp, Trassierung, Verkehrsdichte, Reibwert etc.)[1] unterschieden werden.

[1] Die Liste der die Fahrsituation charakterisierenden Umgebungsmerkmale kann theoretisch beliebig erweitert bzw. verfeinert (z.B. sichteinschränkende Merkmale: Dunkelheit, Nebel, Blendung, etc.) werden. Im Zuge der exemplarischen ASIL-Bestimmung wird sich auf die angegebenen Umgebungsmerkmale beschränkt.

Für die Funktion „Abblendlicht“ relevant (da sichteinschränkend und damit kritisch) sind folgende Merkmale:

- *hell / dunkel → Erst bei Dunkelheit ist die Funktion „Abblendlicht“ zwingend erforderlich.*
- *innerhalb von Ortschaft / außerhalb von Ortschaft → Zu großen Teilen kann davon ausgegangen werden, dass innerstädtische Straßen nachts beleuchtet sind, weswegen ein Versagen der Funktion „Abblendlicht“ dort weniger kritisch ist als außerorts.*
- *hohe Verkehrsdichte / niedrige Verkehrsdichte → Ist die Verkehrsdichte hoch, so kann ein Fahrzeug mit defektem „Abblendlicht“ in einer Kolonne „mitschwimmen“ bzw. sich an anderen beleuchteten Fahrzeugen orientieren.*

4. **Definition der möglichen Fahrzeugzustände**
   Ein funktionaler Fehler des zu bewertenden Systems kann in verschiedenen Fahrzeugzuständen (z.B. Fahrzeug steht, Fahrzeug fährt an, Fahrzeug beschleunigt (positiv/negativ), Fahrzeug fährt mit konstanter Geschwindigkeit) unterschiedliche Risikopotenziale bergen.

Im Falle des Abblendlichtes werden folgende Fahrzeugzustände als betrachtungswürdig identifiziert, da sich hieraus in Kombination mit dem Funktionsfehler kritische Szenarien ergeben können:

- *Fahrzeug fährt an*
- *Fahrzeug beschleunigt stark positiv*
- *Fahrzeug fährt mit hoher konstanter Geschwindigkeit*

5. **Kombination der relevanten Fahrzeugzustände und Fahrsituationen zu Fahrszenarien**
   Durch Kombination der in den vorhergehenden Schritten identifizierten Fahrsituationen mit den unterschiedlichen Fahrzeugzuständen lassen sich für die weitere Betrachtung relevante Fahrszenarien ableiten.

Für das Abblendlicht werden exemplarisch folgende im Detail zu analysierende Szenarien identifziert:

- *Fahrzeug fährt an; bei Dunkelheit, schlechten Sichtbedingungen, innerorts, bei niedriger Verkehrsdichte*
- *Fahrzeug fährt mit hoher Geschwindigkeit; bei Dunkelheit, guten Sichtbedingungen, außerorts, bei niedriger Verkehrsdichte*
- *Fahrzeug beschleunigt stark; Dunkelheit, gute Sichtbedingungen, innerorts, bei niedriger Verkehrsdichte*

6. **Festlegung der möglichen Fehlfunktionen**
   Für das zu bewertende System sind die möglichen funktionalen Fehler (z.B. Komponentenfehler, Bedienfehler, Systemmissbrauch etc.) zu ermitteln. Diese werden in der Praxis häufig mittels einer Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) ermittelt.

Für das Beispiel des Abblendlichtes werden folgende Fehlfunktionen als sicherheitsrelevant eingestuft:

- *Anforderung „Licht ein“ überführt das System nicht in den Zustand „Licht EIN“; Zustand bleibt „Licht AUS“*
- *Licht geht ohne Anforderung „Licht aus“ aus dem Zustand „Licht EIN“ in den Zustand „Licht AUS“*

7. **Bestimmung der Sicherheitsklasse mittels Bewertungsmatrix**
   Um die Sicherheitsklasse der betrachteten Funktion zu bestimmen, ist eine Abschätzung der den ASIL charakterisierenden Parameter *Möglichkeit der Gefahrenabwehr [C] (Controllability)*, *Schadensausmaß [S] (Severity)* und *Aufenthaltswahrscheinlichkeit [E] (Probability of Exposure)* erforderlich (s. Abb. 7.1).
   Hierfür werden dem Anwender der Norm (in ISO 26262-3 Abschnitt 7.4.5) unterschiedliche Klassifizierungshilfen bereitgestellt. Nach den Einzelbewertungen von C, S und E kann für jede betrachtete (Fehl)Funktion im Szenario

die Einstufung in eine Sicherheitsklasse (ASIL) erfolgen. Dies geschieht durch einfache Zuordnung gemäß Tabelle 7.1. Die sicherheitsrelevanten Stufen wer-

Tabelle 7.1: ASIL-Ablesematrix

		Exposure	Controllability		
			C1	C2	C3
Severity	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D
E1: Very low probability E2: Low probability E3: Medium probability E4: High probability		(C0: Controllable in general) C1: Simply controllable C2: Normaly controllable C3: Difficult to control or uncontrollable		(S0: No injuries) S1: Light or moderate injuries S2: Severe and life-threating injuries (survival probable) S3: Life-threatening injuries (survival uncertain); fatal injuries	

den mit ASIL A, B, C und D gekennzeichnet, wobei ASIL A die geringsten und ASIL D die höchsten Sicherheitsanforderungen impliziert. Neben diesen sicherheitsrelevanten Stufen ist in der Matrix die Bezeichnung QM zu finden. QM steht für „Qualitätsmanagement“ und weist darauf hin, dass die untersuchte Funktion explizit keine Sicherheitsfunktion ist und somit das in der Automobilindustrie übliche Qualitätsmanagement ausreichend ist [Pau07].

Die exemplarische Abschätzung der einzelnen den ASIL bestimmenden Parameter für das „Abblendlicht“ ist in Tabelle 7.2 dokumentiert. Unter Verwendung der in Tabelle 7.1 dargestellten Bewertungsmatrix ergibt sich für die zuvor identifzierten (Fehl)Funktionen folgende ASIL-Klassifikation:

- *(Fehl)Funktion: „Licht ein“ überführt System in Zustand „Licht EIN“: ASIL B*
- *(Fehl)Funktion: Licht geht ohne Anforderung „Licht aus“ in den Zustand „Licht AUS“: ASIL B*

Tabelle 7.2: Bestimmung der Sicherheitsklasse

Szenario (Sz) / Fehler (F)		1 Fahrzeug fährt an, bei Dunkelheit, schlechten Sichtbedingungen, innerorts, niedrige Verkehrsdichte	2 Fahrzeug fährt mit hoher Geschwindigkeit, bei Dunkelheit, guten Sichtbedingungen, ausserorts, niedrige Verkehrsdichte	3 Fahrzeug beschleunigt stark, bei Dunkelheit, guten Sichtbedingungen, innerorts, niedrige Verkehrsdichte	Worst case	ASIL B
1	Licht bleibt trotz Anforderung "Licht ein" in Zustand "Licht AUS"	S1	S3	S3	F1/Sz2	ASIL B
		E3	E3	E3		
		C1	C2	C1		
2	Licht geht ohne Anforderung "Licht aus" in Zustand "Licht AUS"	S1	S3	S3	F2/Sz2(3)	ASIL B
		E3	E3	E3		
		C1	C2	C2		

7.2.2 Risikoanalyse nach der Sicherheitsgrundnorm IEC 61508

Entscheidet sich ein Hersteller dafür, sein E/E/PE-Fahrzeugsystem konform den akutell gültigen Normen, und damit gemäß den anerkannten Regeln der Technik zu entwickeln, so bedarf es bezüglich der Gefährdungs- und Risikoanalyse der Erfüllung der in IEC 61508 Teil 1 Abschnitt 7.4 dokumentierten Anforderungen. Diese Anforderungen sind im Vergleich zu den in Abschnitt 7.2.1 dargelegten Anforderungen der ISO 26262 unschärfer formuliert. Hierauf wird in Abschnitt 7.2.3 im Detail eingegangen.
Die IEC 61508 beschreibt im Wesentlichen sehr oberflächlich nachfolgende drei Schritte auf dem Weg zur Bestimmung einer Sicherheitsklasse (SIL). In Klammern wird auf jeweils vergleichbare Schritte aus der ASIL-Bestimmung nach ISO 26262 verwiesen.

1. Gefährdungen und gefährliche Vorfälle der *equipment under control*(EUC) sind (in allen Betriebsarten) für alle vernünftigerweise vorhersehbaren Umstände, einschließlich Fehlanwendung, zu bestimmen. (vgl. Schritt 6 in Abschnitt 7.2.1)

2. Es sind die Abläufe von Ereignissen zu bestimmen, die zu den zuvor identifzierten Gefährdungen und gefährlichen Vorfällen führen können. (vgl. Schritte 3, 4 und 5 in Abschnitt 7.2.1)

3. Es sind die EUC-Risiken zu bestimmen. (vgl. Schritt 7 in Abschnitt 7.2.1)

Zur Umsetzung der beschriebenen Teilaspekte schweigt sich die IEC 61508 im normativen Teil aus. Erst in IEC 61508-5, hierbei handelt es sich um einen rein informativen Teil (vgl. Abschnitt 2.1.2), werden unterschiedliche, sowohl quantitative als auch qualitative Vorgehensweisen zur Bestimmung der Sicherheitsklasse vorgeschlagen.

Dies sind:

- Festlegung der Sicherheits-Integritätslevel über die *Probability of Failure on Demand PFD*(quantitativ)
- Bestimmung der Sicherheits-Integritätslevel mittels *Risikograph* (qualitativ)
- Festlegung der Sicherheits-Integritätslevel mittels *Matrix des Ausmaßes des gefährlichen Vorfalls* (qualitativ)

Im Folgenden wird auf die Risikoklassen-Einstufung von identifzierten Gefährdungen mittels Risikograph (vgl. Abb. 7.2) eingegangen, da hier die größten Überdeckungen zu der in Abschnitt 7.2.1 beschriebenen und in ISO 26262 vorgeschlagenen Methode erkennbar sind.

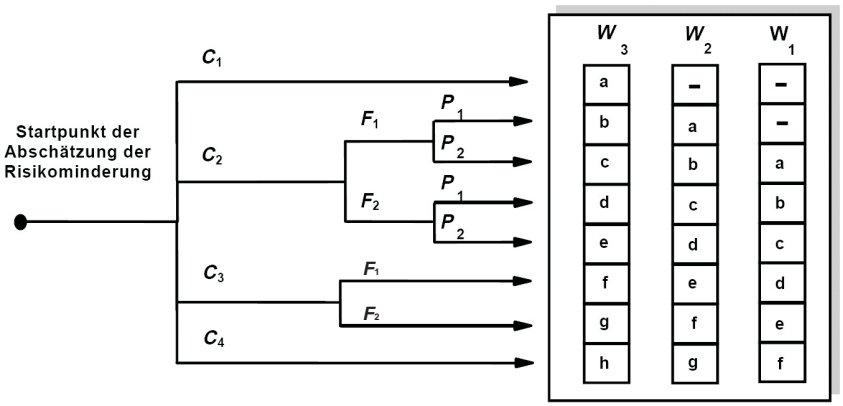


Abbildung 7.2: Risikograph nach IEC 61508 [IEC61508]

Ähnlich wie bei der Einstufung in die automobilen Sicherheitsklassen (ASIL) wird die generische Sicherheitsklasse (SIL) basierend auf der Abschätzung verschiedener Risikofaktoren erreicht.
Die den Risikographen aufspannenden Faktoren stellen sich wie folgt dar:

- Auswirkung eines gefährlichen Vorfalls (C)
- Häufigkeit und Zeit des Aufenthaltes im Gefahrenbereich (F)
- Möglichkeit den gefährlichen Vorfall zu vermeiden (P)
- Wahrscheinlichkeit des unerwünschten Ereignisses (W)

Nach Abschätzung eines jeden Parameters mit Hilfe der in Tabelle 7.3 dargestellten Klassifzierungen kann durch Verfolgen des jeweiligen Pfades indirekt die Sicherheitsklasse der betreffenden Gefährdung bestimmt werden.

Tabelle 7.3: Parameter des Risikographen

Risikoparameter		Klassifizierung
Auswirkung [C]	C_1	geringe Verletzung
	C_2	schwere irreversible Verletzung einer Person oder mehrerer Personen; Tod einer Person
	C_3	Tod mehrerer Personen
	C_4	Tod sehr vieler Personen
Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich [F]	F_1	seltener bis öfterer Aufenthalt im gefährlichen Bereich
	F_2	häufiger bis dauernder Aufenthalt im gefährlichen Bereich
Möglichkeit, den gefährlichen Vorfall zu vermeiden (P)	P_1	möglich unter bestimmten Umständen
	P_2	beinahe unmöglich
Wahrscheinlichkeit des unerwünschten Ereignisses (W)	W_1	Eine sehr geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und nur wenige unerwünschte Ereignisse wahrscheinlich.
	W_2	Eine geringe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und wenige unerwünschte Ereignisse wahrscheinlich.
	W_3	Eine relativ hohe Wahrscheinlichkeit, dass die unerwünschten Ereignisse auftreten, und häufige unerwünschte Ereignisse sind wahrscheinlich.

Hierzu wird die jeweilige notwendige minimale Risikominderung (a-h) im Risikograph abgelesen und mit Hilfe von Tabelle 7.4 das Sicherheitsintegritäts-Level bestimmt.

Tabelle 7.4: Notwendige minimale Risikominderung

Notwendige minimale Risikominderung	**Sicherheitsintegritätslevel**
-	keine Sicherheitsanforderungen
a	keine speziellen Sicherheitsanforderungen
b,c	1
d	2
e,f	3
g	4
h	E/E/PES-Sicherheitssystem reicht nicht aus

Die SIL-Einstufung mittels Risikograph wird im Folgenden für die bekannte Beispielfunktion „Abblendlicht“ aufgezeigt.
Werden die Gefährdungen bzw. gefährlichen Vorfälle zur besseren Vergleichbarkeit analog zu der in Abschnitt 7.2.1 beschriebenen Vorgehensweise ermittelt, kann beispielsweise die Sicherheitsklasse für die Fehlfunktion:

> *Anforderung „Licht ein“ überführt das System nicht in den Zustand „Licht EIN“; Zustand bleibt „Licht AUS“*

mittels des in Abbildung 7.2 dargestellten Risikographen bestimmt werden.
Hierfür werden die Risikoparameter mit Hilfe von Tabelle 7.3 in Anlehnung an die Schätzungen aus Abschnitt 7.2.1 geschätzt. Hierbei wird explizit nur von einer *Anlehnung* gesprochen, da die Parameter, auf welchen die Risikobewertungen nach ISO 26262 und IEC 61508 beruhen, nicht alle direkt vergleichbar sind.

- Auswirkung: C_2 [ISO 26262: S3]
- Häufigkeit u. Aufenthaltsdauer im gefährlichen Bereich: F_2 [ISO 26262: -]
- Möglichkeit, den gefährlichen Vorfall zu vermeiden: P_2 [ISO 26262: C2]
- Wahrscheinlichkeit des unerwünschten Ereignisses: W_3 [ISO 26262: -]

Die Parameter C und P (nach IEC 61508) sind gut vergleichbar mit den Parameter S und P (nach ISO 26262). Im Falle der Parameter F und W (nach IEC 61508) lassen sich keine direkten Korrelate (s. auch Abschnitt 7.2.3) identifzieren („-“). Diese Parameter gilt es unter Verwendung von Tabelle 7.3 losgelöst von den Werten aus Abschnitt 7.2.1 zu schätzen.

Durch Nachverfolgung der Pfade des Risikographen (s. Abbildung 7.2) lässt sich eine notwendige minimale Risikominderung von „e“ bestimmen, so dass sich unter Verwendung von Tabelle 7.4 für das „Abblendlicht“ eine Sicherheitsklasse von SIL 3 ergibt.
Abbildung 7.3 zeigt, dass eine direkte Überführung von der generischen Sicherheitsklasse (SIL) in die automobilspezifische Sicherheitsklasse (SIL) nicht immer eindeutig möglich ist. So kann eine SIL 2-Funktion theoretisch sowohl in eine ASIL B-,

als auch eine ASIL C-Funktion überführt werden (vgl. a)). Gleiches gilt für die umgekehrte Überführung (vgl. b). Auch hier ist keine eindeutige Zuordnung definiert. Vor diesem Hintergrund und aufgrund der mehrfach kritisierten sehr subjektiven

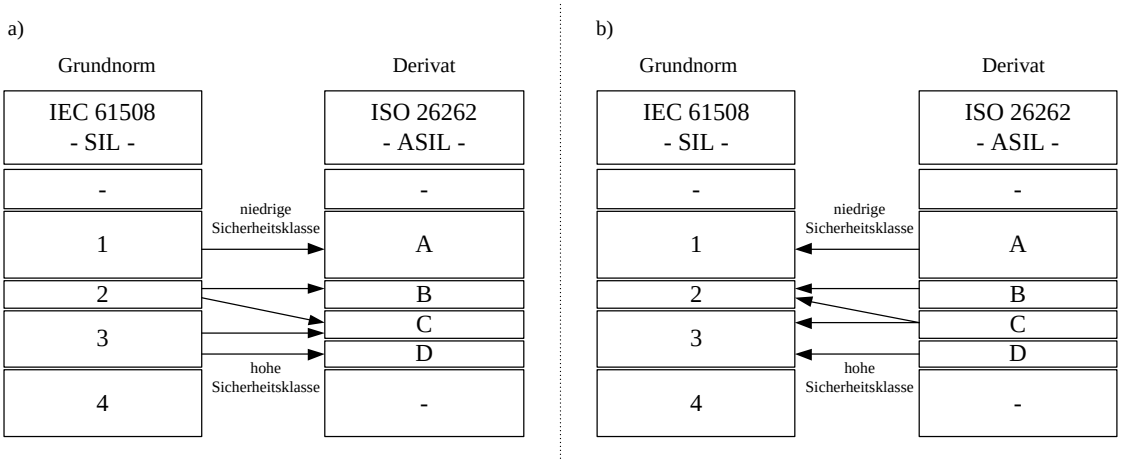


Abbildung 7.3: ASIL-SIL-Überführung [b) basierend auf [Go09]]

Schätzungen der einzelnen Parameter, soll im Folgenden nicht weiter diskutiert werden, warum die unterschiedlichen Ansätze zu abweichenden Ergebnissen (ISO 26262: ASIL B; IEC 61508: SIL 3) führen.
Da die Risikoanalyse nach ISO 26262 im Mittelpunkt dieser Untersuchung steht, wird zur Validierung des EmMORI-Ansatzes jeweils nur noch auf die in Abschnitt 7.2.1 vorgestellte ASIL-Einstufung zurückgegriffen.

7.2.3 Gemeinsamkeiten und Unterschiede der Risikoanalyse nach IEC 61508 und ISO 26262

In den Abschnitten 7.2.1 und 7.2.2 werden die Vorgehensweisen zur Gefährdungs- und Risikoanalyse vorgestellt, wie sie in ISO 26262 und IEC 61508 vorgeschlagen werden. Zur besseren Nachvollziehbarkeit wurden beide Methoden exemplarisch zur Bestimmung der Sicherheitsklasse auf ein und dieselbe Beispielfunktion „Abblendlicht“ angewendet.
Im Folgenden sollen basierend auf den vorhergehenden Ausführungen die wesentlichen Gemeinsamkeiten und Unterschiede der verschiedenen Ansätze aufgezeigt und diskutiert werden.
Bereits der Vergleich der Verortung und des Umfanges der die Gefährdungs- und

Risikoanalyse enthaltenen Normen-Abschnitte verdeutlicht, dass dieser Analyse in der ISO 26262 ein wesentlich höherer Stellenwert zugewiesen wird, als dies in IEC 61508 der Fall ist.
So werden die unterschiedlichen Aspekte der Gefährdungs- und Riskikoanalyse sehr detailliert und normativ in ISO 26262-3 beschrieben, und dem Anwender der Norm wird ein strukturierter Leitfaden zur Bestimmung der Sicherheitsklasse (ASIL) an die Hand gegeben.
Die IEC 61508 dagegen beschreibt im normativen Teil 1 lediglich, dass eine Gefährdungs- und Risikoanalyse durchgeführt werden muss. Wie im Detail vorzugehen ist, wird dem Anwender im normativen Teil selbst überlassen. Auch im rein informativen Teil 5 der Norm, auf welchen verwiesen wird, werden die verschiedenen Teilschritte der Analyse, abgesehen von der abschließenden Bestimmung der Sicherheitsklasse, nicht im Detail erläutert.
Zur Bestimmung der Sicherheitsklasse (SIL) werden dem Anwender der IEC 61508 wie in Abschnitt 7.2.2 beschrieben drei unterschiedliche Vorgehensweisen angeboten. Hier ist die ISO 26262 wesentlich konsequenter, indem sie ein Verfahren normativ vorgibt.
Werden explizit die unterschiedlichen in ISO 26262 und IEC 61508 beschriebenen Verfahren zur abschließenden Bestimmung einer Sicherheitsklasse verglichen, so ist festzustellen, dass der ASIL nach ISO 26262 auf der Schätzung von drei Parametern, der SIL nach IEC 61508 aber auf der Schätzung von vier Parametern basiert. Zudem unterscheiden sich auch die Anzahl und das Wesen der für den jeweiligen Parameter zu verwendenden Klassen und deren ordinale Quantifizierungen.
Mit dem Parameter „Schadensausmaß“ nach ISO 26262 und dem Parameter „Konsequenz“ nach IEC 61508 können die Folgen bzw. Konsequenzen eines Schadensereignisses analog bewertet werden. In beiden Fällen wird dem Anwender eine vierstufige Ordinal-Skala bereit gestellt. Der wesentliche Unterschied ist, dass im Falle der Anwendung der IEC 61508 mit den Klassen C3 und insbesondere C4 auch Großschäden bzw. katastrophale Unfälle bewertet werden können, bei denen eine Vielzahl von Todesopfern zu erwarten ist. Solch katastrophale Unfälle können in der Regel nicht von einem im Fahrzeug (ISO 26262 adressiert lediglich Personenkraftwagen bis 3,5 t zulässiges Gesamtgewicht → d.h. Busse, Lastkraftwagen ausgeschlossen) verbauten E/E/PE-System verursacht werden, weswegen sich die ISO 26262 in der Klasse S3 auf „Schwere Verletzungen bis Tote“ beschränkt.

Soll die Wahrscheinlichkeit der Exposition in einer bestimmten Fahrsituation bewertet werden, so wird gemäß ISO 26262 der Parameter E verwendet. In der IEC 61508 ist kein direktes Korrelat zu finden. IEC 61508 unterscheidet vielmehr zwischen einer „Häufigkeit und Aufenthaltsdauer im Gefahrenbereich“ und einer „Wahrscheinlichkeit des unerwünschten Ereignisses“. Diese Unterscheidung ist aus Sicht eines Automobil-Herstellers/-Zulieferers wenig sinnvoll, da sich der Fahrer eines Straßenfahrzeuges quasi während der gesamten Betriebsdauer im Gefahrenbereich „Straßenfahrzeug“ befindet. Die in ISO 26262 verankerte „Wahrscheinlichkeit bzw. Aufenthaltsdauer in einer Fahrsituation“ kann hier eher als eine indirekte Kombination aus den in IEC 61508 dokumentierten Parametern *Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich* (F) und *Wahrscheinlichkeit des unerwünschten Ereignisses* (W) verstanden werden.
Die zur Bewertung der Möglichkeit der Gefahrenabwehr hinzugezogenen Parameter „C“ und „P“ sind gut vergleichbar. Hier liegt der Unterschied lediglich darin, dass die Möglichkeit der Gefahrenabwehr bei Anwendung der ISO 26262 aufgrund der höheren Trennschärfe (4 statt 2 Klassen) granularer bewertet werden kann.
Die wesentlichen Unterschiede der risikoanalyserelevanten Inhalte der IEC 61508 und des ISO 26262 sind in Tabelle 7.5 zusammengefasst.

Tabelle 7.5: Normativer Vergleich von Risikoanalysen

Vergleichsmerkmal		IEC 61508	ISO 26262
Verortung		In den normativen Teilen wird lediglich darauf hingewiesen, dass eine Risikoanalyse durchgeführt werden soll; Details werden dem Anwender erst im informativen Anhang geliefert	Detaillierte Beschreibung des formalen Vorgehens bei "Hazard analysis and risk assessment"
Sicherheitsklassen		SIL: eine von vier diskreten Stufen zur Spezifizierung der Anforderung für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/PE-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt	ASIL: one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures for avoiding an unreasonable residual risk with D representing the most stringent and A the least stringent level
Methoden zur Bestimmung der Sicherheitsklasse		Festlegung der Sicherheits-Integritätslevel über die Probability of Failure on Demand PFD (quantitativ)	"Hazard classification" gemäß ISO 26262:3; 7.4.5
		Bestimmung der Sicherheits-Integritäts-level mittels Risikograph (qualitativ)	
		Festlegung der Sicherheits-Integritäts-level mittels Matrix des Ausmaßes des gefährlichen Vorfalls (qualitativ)	
Parameter	Konsequenz/ Schadensausmaß	Auswirkung [C]	Severity of potential harm [S]
	Aufenthalts-wahrscheinlichkeit	Häufigkeit und Aufenthaltsdauer im gefährlichen Bereich [F]	Probability of Exposure regarding operational situations [E]
		Wahrscheinlichkeit des unerwünschten Ereignisses [W]	
	Kontrollierbarkeit	Möglichkeit den gefährlichen Vorfall zu vermeiden [P]	Controllability [C]
Kategorien von	Konsequenz/ Schadensausmaß	C1: geringe Verletzung C2: schwere irreversible Verletzung einer oder mehrerer Personen; Tod einer Person C3: Tod mehrerer Personen C4: Tod sehr vieler Personen	S0: no injuries S1: light and moderate injuries S2: sever injuries, possibly life-threatenig S3: life-threatening injuries or fatal injuries
		DELTA: Mittels der Kategorien für das *Schadensausmaß* nach IEC 61508 können auch Großschäden/Katastrophen bewertet werden. Die höchste Schwerekategorie nach ISO 26262 lässt lediglich auf das Potenzial von schweren Verletzungen und/oder einzelnen Toten schließen.	
	Aufenthalts-wahrscheinlichkeit	DELTA: Die Aufenthaltswahrscheinlichkeit wird im Sinne der IEC 61508 durch zwei Parameter (vgl. Parameter) aufgespannt. Nach ISO 26262 wird die *Wahrscheinlichkeit des Aufenthalts in einer Fahrsituation* direkt abgeschätzt.	
	Kontrollierbarkeit	P1: möglich unter bestimmten Bedingungen P2: beinahe unmöglich	C0: controllable in general C1: simply controllable C2: normally controllable C3: difficult to control or uncontrollable
		DELTA: Die Möglichkeit der Kontrolliebarkeit einer Situation wird nach ISO 26262 feingranularer unterschieden als nach IEC 61508.	

Kapitel 8

EmMORI-Methode – Modellbildung, -simulation und -analyse

Wie in Abschnitt 1.1 formuliert ist es nicht Ziel dieser Arbeit, mit der in ISO 26262 beschriebenen Methode zur Gefährdungs- und Risikoanalyse (s. Abschnitt 7.2.1) in Konkurrenz zu treten, sondern vielmehr deren Ergebnisse durch eine modellbasierte Erweiterung zu objektivieren und zu konkretisieren.
Objektivierende Ansätze können in der Regel immer dort gewinnbringend eingesetzt werden, wo die Analyse stark von subjektiven Meinungen (vgl. Abschnitt 5.1.10) des die Risikoanalyse durchführenden Personenkreises abhängig ist. Eben diese Voraussetzung ist im Falle der Gefährdungs- und Risikoanalyse gemäß ISO 26262 im Zuge der Gefährdungsklassifikation und der sich anschließenden Zuordnung einer Sicherheitsanforderungsstufe (vgl. Abbildung 8.1: Risikoeinschätzung), dem Automotive Safety Integrity Level, gegeben.
Nach ISO 26262 sollen sämtliche in den vorhergehenden Phasen (s. Abschnitt 7.2.1) identifzierten Gefährdungen hinsichtlich ihres potenziellen Schadensausmaßes (S), der Wahrscheinlichkeit der Exposition im jeweiligen Fahrszenario (E) und der Kontrollierbarkeit (C) der gefährlichen Situation durch den Fahrer oder durch andere Verkehrsteilnehmer geschätzt werden.
Mit Hilfe des hier dargestellten Ansatzes sollen diese Schätzungen, soweit dies unter den gegebenen Voraussetzungen möglich ist, mittels Simulation und Analyse von Petrinetzen objektiviert werden.
Voraussetzung hierfür ist ein strukturierter Modellbildungsprozess, um eine kondensierte Sicht auf die, die einzelnen Parameter beinflussenden, abstrakten Faktoren zu

erhalten [SPP03, Sch99b]. Auch wenn in der Simulation dieser Modelle der eigentliche Hauptnutzen besteht, können mittels strukturierter Modellierung von Systemen etc. weitere positive Effekte erzielt werden. Pizka etc. heben in [SPP03] insbesondere

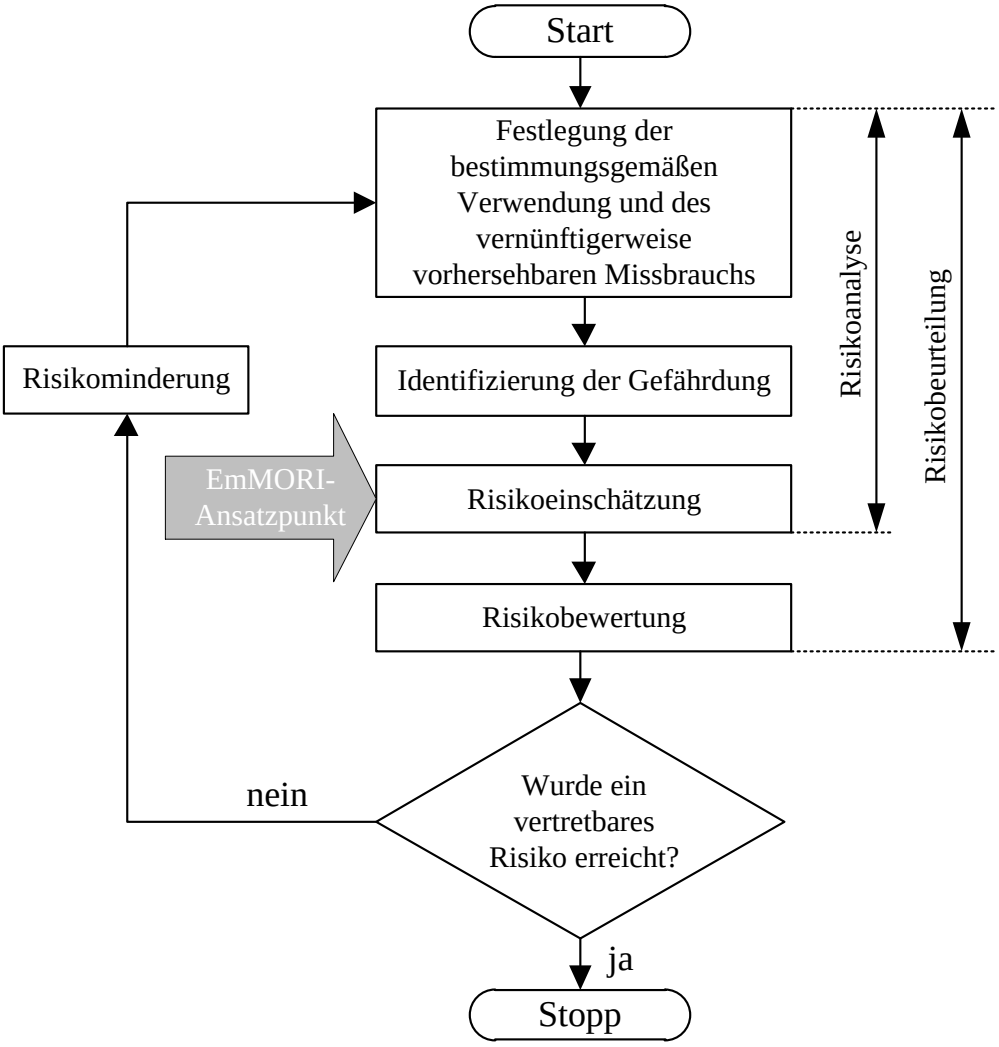


Abbildung 8.1: Schritte einer Risikobetrachtung nach DIN Fachbericht 144 [DIN FB 144]

ein besseres System-/Funktions-Verständnis (von z.B. Anforderungen, Randbedingungen etc.), eine verbesserte Kommunikation (zwischen z.B. System-Entwicklern und Risikoanalysten) und einen höheren Grad an automatisierter Prüfbarkeit (z.B. Konsistenz- und Korrektheitsprüfungen) hervor.

8.1 Parameter mit Objektivierungspotenzial

Gilt es ein System bzw. eine Funktion konform ISO 26262 zu entwickeln, so sind auch bei Anwendung des vorgeschlagenen Ansatzes weiterhin dessen Anforderungen bzgl. der Risikoanalyse (vgl. Abschnitt 7.2.1) zu erfüllen. Die objektivierende Wirkung des Ansatzes kann lediglich bei der Abschätzung der ASIL-Parameter unterstützen. Hierfür ist nachvollziehbarerweise ein detailliertes Verständnis der die einzelnen ASIL-Parameter beeinflussenden Faktoren erforderlich. Die Basis für dieses grundlegende Verständnis wird in den Abschnitten 8.1.1 bis 8.1.3 geschaffen, bevor abschließend deren Möglichkeit der modellgestützen Objektivierung diskutiert (s. Abschnitt 8.2) wird.

8.1.1 ASIL-Parameter Schadensausmaß

> **Severity:** [nach ISO 26262-1]
> Measure of the extent of harm to an individual in a specific situation.

Nach ISO 26262-1 wird das Schadensausmaß bewertet, welches sich in einer bestimmten Situation für ein potenziell gefährdetes Individuum ergeben kann. Potenziell gefährdete Individuen können hierbei sowohl Fahrzeuginsassen als auch andere Verkehrsteilnehmer (z.B. Radfahrer, Fußgäner oder Insassen anderer Fahrzeuge) sein. Die Klassifikation des Schadensausmaßes ist auf einer Ordinal-Skala von S0 (keine Verletzte, aber ggf. materielle Schäden) bis S3 (lebensbedrohliche Verletzungen, Tote) möglich.
Zur besseren Abschätzung des Schadensausmaßes wird dem Anwender der Norm empfohlen Bewertungsskalen (z.B. AIS, ISS, NISS etc.) für die Schwere von Einzelverletzungen zu nutzen, mit Hilfe welcher sich eine Überlebenswahrscheinlichkeit ableiten lässt.
Problematisch ist hierbei, dass diese Skalen in der Regel stark vom *Stand der Medizin* zu dem Zeitpunkt abhängig sind, zu dem die Analyse durchgeführt wird, und damit über die Zeit variieren [ISO26262]. Trotz dieses zeitlichen Wandels der Bewertungsskalen wird dem Anwender der Norm mit diesen ein geeignetes Hilfsmittel an die Hand gegeben, um die Schätzaufgabe zu erleichtern und in gewissem Maße zu objektivieren. Weiteres Objektivierungspotenzial sieht der Autor in der Simulation

von Modellen, welche Verunfallungsszenarien und die daraus resultierenden Schadensereignisse abbilden.
Im Zuge der Umsetzung dieses Objektivierungsansatzes des Parameters S ist jedoch insbesondere die Modellkomplexität zu diskutieren, welche sich bei der realitätsnahen Abbildung von komplexen Unfallszenarien einstellt, welche den Parameter S maßgeblich mitbestimmen.
So ist das Schadensausmaß mindestens von den in Abbildung 8.2 in Anlehnung an ein Klassendiagramm der UML dargestellten Faktoren abhängig.

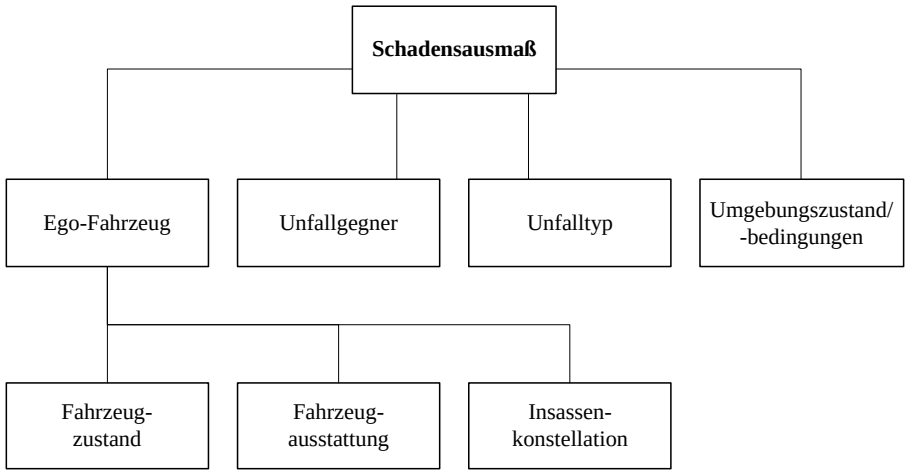


Abbildung 8.2: Einflussfaktoren auf das Schadensausmaß

Diese Aspekte gehen zwar zum Teil auch schon in die in ISO 26262 vorgeschlagenen Bewertungsskalen ein, werden jedoch wie die nachstehende Argumentation aufzeigt und ISO 26262 selbst formuliert noch zu oberflächlich behandelt, um valide objektive Aussagen treffen zu können.

Schadensausmaß in Abhängigkeit vom Ego-Fahrzeug: Das aus einem Schadensereignis resultierende Schadensausmaß ist in hohem Maße abhängig von den in Abbildung 8.2 zusammengefassten dem Ego-Fahrzeug innewohnenden Faktoren.
So wird zwar in ISO 26262:3 Annex B auch zwischen Unfällen bei verschiedenen Differenzgeschwindigkeiten unterschieden, der aktuelle Geschwindigkeitsbereich (z.B. in Abhängigkeit vom Straßentyp/-zustand) und/oder der kurz vor dem Unfall vorherrschenden Beschleunigungszustand wird jedoch vernachlässigt.

Das auch die jeweilige Fahrzeugausstattung des Ego-Fahrzeuges mit aktiven und/oder passiven Sicherheitssystemen (z.B. Airbags) einen erheblichen Einfluss auf das Schadensausmaß hat, steht außer Frage. Trotzdem wird der Aspekt der Fahrzeugausstattung in der ISO 26262 gerade einmal mit nachstehender Anmerkung (ISO 26262-3; 7.4.3, Note 1) abgehandelt:

> „In the evaluation of an item, there can be benefits from other items such as airbags, if those items are sufficiently independent."

In den nach ISO 26262 bei der Einschätzung von Schadensausmaßen hinzuzuziehenden exemplarischen Schadensausmaß-Klassifikationen sind hierzu keine Hinweise gegeben.
Des Weiteren ist das Schadensausmaß nachvollziehbarerweise immer auch von der Insassenkonstellation und sogar der Konstitution der einzelnen Insassen abhängig. So zeigen unterschiedliche Studien, dass die biomechanischen Belastungsgrenzen von Fahrzeuginsassen in Abhängigkeit von individuellen Aspekten wie Geschlecht, Alter, Gewicht etc. erheblich streuen [BGK+09], was zur Folge hat, dass auch das Schadensausmaß in weiten Grenzen variieren kann. Dieser Tatsache ist es auch geschuldet, dass sich ein eigenes Forschungsgebiet mit der Insassensimulation beschäftigt [MS09].

Schadensausmaß in Abhängigkeit vom Unfallgegner: In ISO 26262:3 Annex B werden Kollisionen mit unterschiedlichen Unfallgegnern (z.B. truck, pedestrian) hinsichtlich des resultierenden Schadensausmaßes eingestuft. Dieser Aspekt des je nach Unfallgegner stark variierenden Schadenspotenzials bedarf jedoch insbesondere vor dem Hintergrund der Vielzahl von unterschiedlichen potenziellen Unfallgegnern (vgl. Tabelle 8.1) einer detaillierteren Betrachtung. Theoretisch lässt sich diese an [BM09] angelehnte potenzielle Unfallgegner auflistende Tabelle über den Bereich der Straßenfahrzeuge hinaus auch in Richtung weiterer Straßenverkehrsteilnehmer (z.B. Radfahrer, Fussgänger), Fahrzeuge anderer Verkehrsträger (z.B. Schienenfahrzeug (z.B. Eisenbahn an Bahnübergang, Straßenbahn im Innenstadtbereich)) und statische Infrastruktur-Elemente erweitern.
Zudem ist für eine realistische Abschätzung des Schadensausmaßes wieder die Insassenkonstellation und -konstitution (s. oben) der verschiedenen am Unfall beteiligten Fahrzeuge von Interesse.

Tabelle 8.1: Kraftfahrzeug-Typen nach [BM09] (Auszug)

Straßenfahrzeug	**Definition, Beispiele**
Motorrad	Einspuriges Kfz mit 2 Rädern, eventuell mit Beiwagen; mit festen Fahrzeugteilen (z.B. Tank) im Kniebereich
Limousine	Personenkraftwagen mit geschlossenem Aufbau und maximal 4 Seitentüren
Kabriolett	Personenkraftwagen mit offenem Aufbau, eventuell mit Überrollbügel, 2 oder 4 Türen
Reisebus	Nutzkraftwagen zum Transport von Personen im Langstreckenverkehr, keine Stehplätze
Sattelzugmaschine	Nutzkraftwagen zum Ziehen von Sattelanhänger
Traktor	Nutzkraftwagen; Zugmaschine, auch zum Schieben, Tragen oder Antreiben von auswechselbaren Geräten

Schadensausmaß in Abhängigkeit vom Unfalltyp: Auch der Einfluss des Unfalltyps/-szenarios auf das Schadensausmaß hat mit Annex B rudimentär Einzug in das Automotive-Derivat der IEC 61508 Einzug erhalten. Im Hinblick auf eine realitätsnahe Bewertung verschiedener Unfallszenarien hinsichtlich des von ihnen ausgehenden Schadensausmaßes fehlt jedoch der Bezug zu strukturierten Unfalltypenkatalogen (z.B. Karlsruher Unfalltypenkatalog).

Schadensausmaß in Abhängigkeit vom Umgebungszustand: Dem Einfluss der Umgebungsbedingungen auf das Schadensausmaß wird in ISO 26262 keine Beachtung geschenkt. Dies möglicherweise aufgrund des direkten Zusammenhangs zwischen den vorherrschenden Umgebungsbedingungen und einem sich einstellenden Unfallereignis bzw. Unfalltyp mit seinem resultierendem Schadenspotenzial.
Trotzdem soll hier darauf hingewiesen werden, dass das Schadensausmaß beispielsweise auch von Reibwertveränderungen beeinflusst wird. Dies wird u.a. in verschiedenen Untersuchungen zum Rollover deutlich. Diese zeigen, dass es bei ungünstigen Umgebungs-/Straßenbedingungen in Kurven zu kraftschlussbedingtem Kippen von Fahrzeugen mit hohem Schwerpunkt kommen kann, da hier ein Zielkonflikt zwischen ausreichender Kippsicherheit und Kurvenstabilitätsreserven vorliegt [Bau03].

Zusammenfassung – Schadensausmaß

Die vorausgehenden Abschnitte zeigen auf, dass das Schadensausmaß von einer Vielzahl von egofahrzeugimmanenten (z.B. Bewegungszustand, Fahrzeugausstattung, Insassenkonstellation) und von, vom Ego-Fahrzeug losgelösten (z.B. Unfallgegner) Faktoren abhängig ist. Zudem wird das Schadensausmaß von Faktoren beeinflusst, welche von einander abhängig sind (z.B. Unfalltyp). So wird beispielsweise die Kollision eines mit $30km/h$ fahrenden Fahrzeuges mit einem Infrastrukturelement ($v_{Infrastruktur} = 0km/h$) ein ganz anderes Schadensbild, und damit auch Schadensausmaß, mit sich bringen, als bei gleicher Geschwindigkeit der Frontalzusammenstoß mit einem ebenfalls 30 km/h schnell fahrenden Reisebus.

8.1.2 ASIL-Parameter Expositionswahrscheinlichkeit

(Probability of) Exposure: [nach ISO 26262-1]
State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis.

Gemäß der vorstehenden Definition gilt es die Wahrscheinlichkeit des Aufenthaltes bzw. der Aussetzung in einem Fahrszenario abzuschätzen, welches bei gleichzeitigem Auftreten der betrachteten Fehlfunktion potenziell zu einem gefährlichen Ereignis und nachfolgendem Schaden führen kann.
Die verschiedenen zu betrachtenden Szenarien lassen sich in Anlehnung an den in [Hör04] gezeigten Ansatz zur Dekomposition von Funktionen wie folgt dekomponieren (vgl. Abbildung 8.3).
Ein jedes *Fahrszenario* wird durch die Kombination eines Umgebungszustandes (*Situation*) und eines *Fahrzeug-Zustandes* zusammengesetzt.
Sowohl Umgebungszustand als auch Fahrzeugzustand werden soweit verfeinert, dass generische, den Umgebungs- bzw. den Fahrzeugzustand beschreibende Merkmale identifiziert werden können.
Jedes dieser Merkmale kann theoretisch unendlich viele unterschiedliche Merkmalsausprägungen einnehmen. Die (Fahr-)Situation wird inbesondere durch die verschiedenen Umgebungseinflüsse, der Fahrzeugzustand dagegen durch den jeweiligen Bewegungszustand des Fahrzeuges charakterisiert.

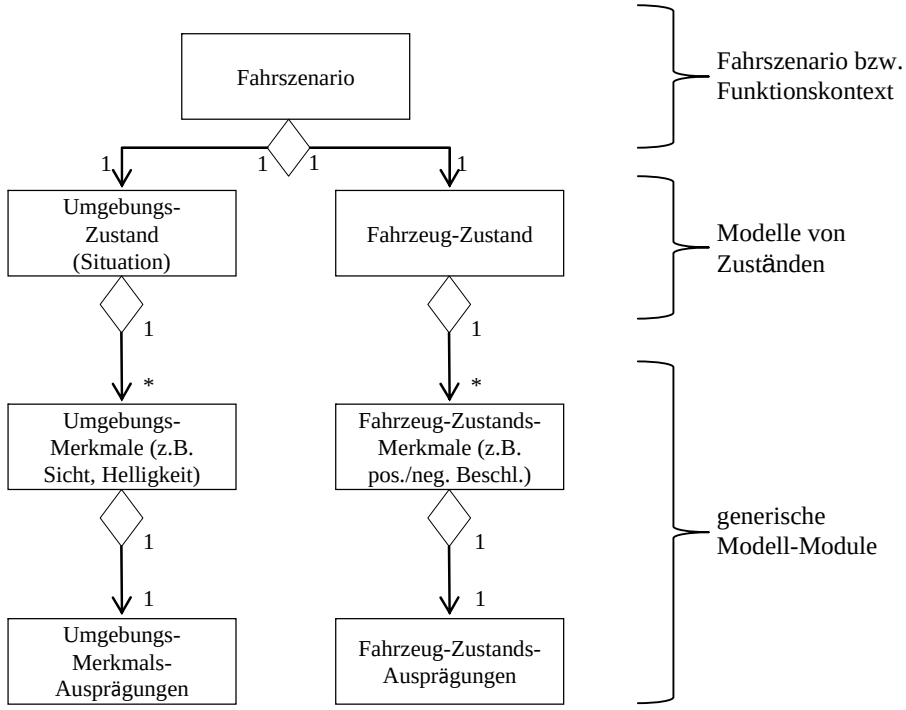


Abbildung 8.3: (De-)Komposition von Fahrszenarien (in Anlehnung an [Hör04])

In ISO 26262-3 Anhang B sind nachfolgende Beispiele[1] gegeben.

- (Fahr-)Situation
  - Verortung des Fahrzeuges (z.B. Autobahn, Landstraße, Garage, Tunnel)
  - Objekte auf der Fahrbahn (z.B. andere Fahrzeuge, Gegenstände)
  - Oberflächenbeschaffenheit (z.B. Nässe, Schnee, Eis)
  - Umweltbedingungen (z.B. Nebel, Regen)
- Fahrzeugzustand
  - Fahrzeuggeschwindigkeit bzw. -beschleunigung

Allein die Kombinatorik möglicher Fahrsituationen und Fahrzeugzustände verdeutlicht die hohe Komplexität der vom Risikoanalysten zu bewältigenden Schätzaufgabe. Zusätzlicher Schätzaufwand ergibt sich, wenn ein und dasselbe System für teil-

[1]Eine Vielzahl der Beispiele sind explizit in den Tabellen in ISO 26262-3 Anhang B beschrieben. Einige zusätzliche Beispiele sind implizit enthalten (z.B. Parken $\rightarrow$ Fahrzeug steht ($v = 0$), Anfahren $\rightarrow$ Fahrzeug fährt langsam ($v < 10km/h$).

weise vollkommen unterschiedliche Märkte – mit verschiedenen Kundentypen (z.B. Stadtfahrer vs. Überlandfahrer) und/oder verschiedenen Umgebungseinflüssen (z.B. Nordschweden (langanhaltend niedrige Temperaturen) vs. Süditalien (Hitzewellen)) – zugelassen werden soll (vgl. Zitat).

> **Estimation of the probability of exposure in the operational situations** → NOTE 3 The exposure determination is based on a representative sample of customers for the target markets [ISO DIS 26262: 7.4.5.3]

8.1.3 ASIL-Parameter Kontrollierbarkeit

> **Controllability:** [nach ISO 26262-1]
> Avoidance of the specified harm or damage through the timely reactions of the persons involved.

Unter der Kontrollierbarkeit wird nach ISO 26262 die mögliche Gefährdungsabwehr aller beteiligten Individuen verstanden. Mittels dieses Parameters wird sowohl die Möglichkeit der Gefährdungsabwehr durch den Fahrer, als auch durch weitere vom System gefährdete Personen (z.B. andere Verkehrsteilnehmer) bewertet.
Die Kontrollierbarkeit wird stark vom *Umgebungszustand* bzw. den *Umgebungsbedingungen*, aber auch von der Einschätzung des Umgebungszustandes durch die beteiligten Individuen, deren *Fähigkeiten*, deren persönlichem *System- bzw. Funktionsverständnis* (vgl. ISO DIS 26262-3; 7.4.5.4.1, Note 2) und den ihnen zur Verfügung stehenden die Kontrollierbarkeit verbessernden technischen Systemen (z.B. ESP) beeinflusst. Der Zustand des Fahrers und seine Befähigung werden zu Analysezwecken nach ISO 26262 vereinfachend wie folgt angenommen.

> „Der Fahrer ist in angemessener Verfassung ein Fahrzeug zu steuern, hat eine gültige Lizenz ein Kraftfahrzeug zu führen und hält sich an die gesetzlichen Regelungen."

In den nachfolgenden Abschnitten wird die Sinnhaftigkeit dieser Vereinfachung hinterfragt und die Möglichkeit einer modellbasierten Objektivierung der Abschätzung des Parameters *Kontrollierbarkeit* diskutiert. Die sehr flexible Formulierung des zu

Analysezwecken angenommenen Fahrerzustandes weist bereits auf eine gewisse Problematik bei der Abschätzung der Kontrollierbarkeit hin und bietet Nährboden für subjektive Einflüsse. So lässt die Anforderung „driver has a driver's license" noch keinen Einblick in das tatsächliche Fahrvermögen des Fahrers zu, zumal die Fahrausbildung (vgl. Abb. 8.4), hier festgemacht an den Ausbildungskosten, von Staat zu Staat sehr unterschiedliche Ausbildungsumfänge beinhaltet.

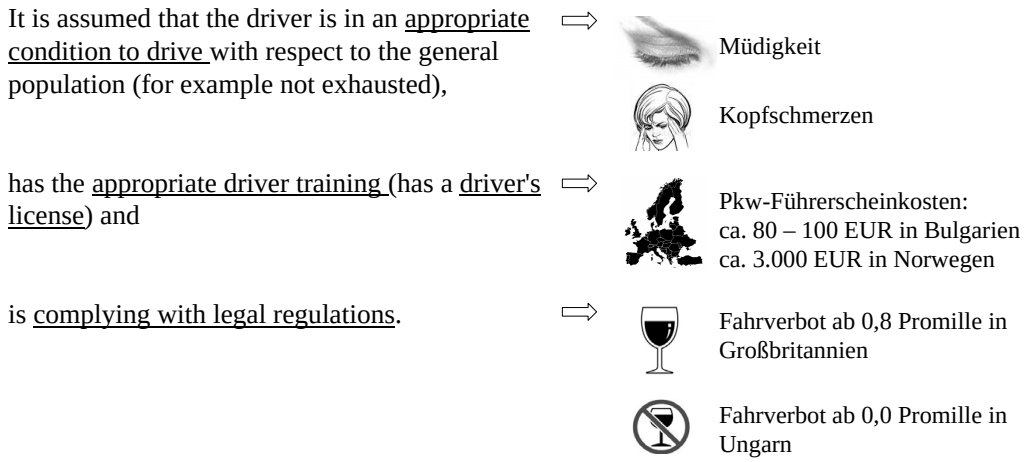


Abbildung 8.4: Vagheit der Fahrer-Konstitution und -Ausbildung [Aut09, OEA09]

Zudem sei hier angemerkt, dass sich ISO 26262 mit ihren Beispielen (s. ISO DIS 26262-3; Annex B, Table 4) hinsichtlich der Befähigung eine Situation zu kontrollieren ausschließlich auf Fahrer bezieht. Andere Verkehrsteilnehmer, deren Möglichkeit eine Gefährdungssituation (s. Anforderung in ISO) abzuwenden gleichermaßen bewertet werden soll (vgl. Zitat), werden hier nicht näher spezifiziert.

> The controllability of each hazardous event, by the driver or other traffic participants, shall be estimated. [ISO DIS 26262-3; 7.4.5.4.1]

Vor diesem Hintergrund wird im Folgenden analysiert, welche Faktoren den Parameter Kontrollierbarkeit beeinflussen und inwiefern diese zur Objektivierung in simulationsfähigen Modellen realistisch abbildbar sind.

Als wesentliche die Kontrollierbarkeit beeinflussenden Faktoren werden die in Abbildung 8.5 dargestellten eingestuft.

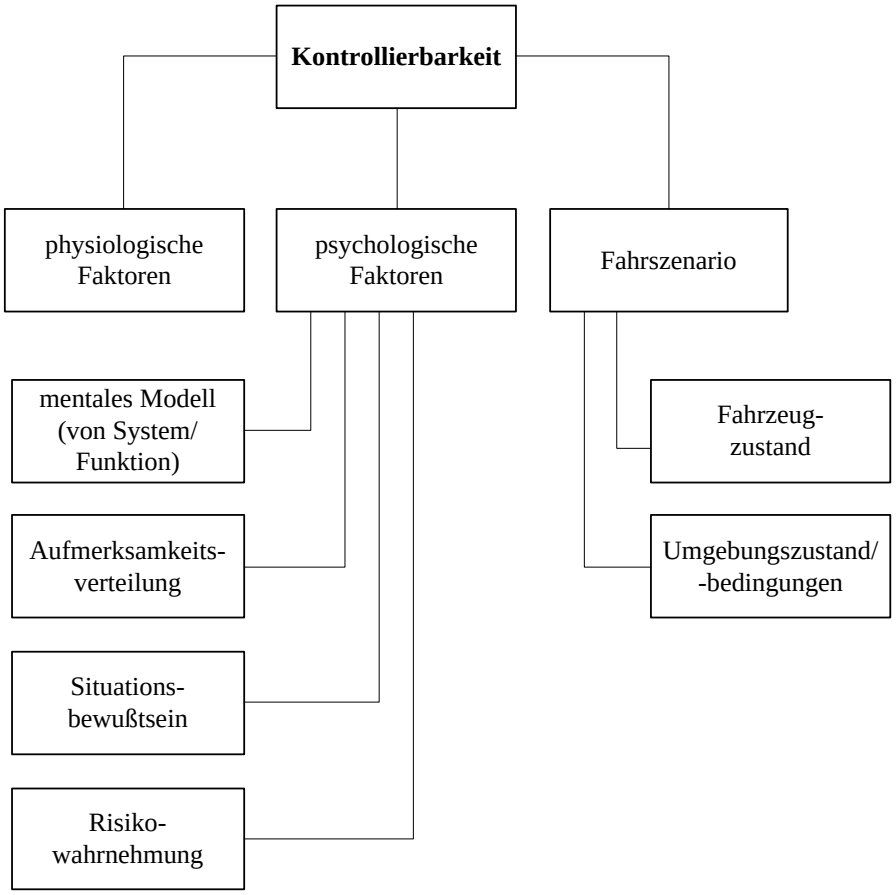


Abbildung 8.5: Einflussfaktoren auf die Kontrollierbarkeit

Eine Gefährdungssituation ist durch das zeitliche und räumliche Aufeinandertreffen einer potentiellen Gefahr mit den zu schützenden Rechtsgütern definiert. Im Falle der Bewertung der Kontrollierbarkeit gilt es die menschlichen Rechtsgüter, also den Fahrzeugführer und sämtliche der Gefährdungssituation ausgesetzten Individuen (z.B. Radfahrer, Fußgänger etc.), welche diese Gefährdungssituation durch eine Aktion beeinflussen können, zu analysieren.
Hierbei reicht es nach [Wer06] nicht aus das Verhalten der Menschen allein auf ein regelungstechnisches Modell zu reduzieren. Es müssen auch seine kognitiven Leistungen, sowie sein Problemlösungs- und Entscheidungsverhalten und seine physische Konstitution (die Komplexität dieses Aspektes wurde bereits in Abschnitt 8.1.1 be-

leuchtet) berücksichtigt werden.
Vielfach wird davon ausgegangen, dass sich Individuen ein mentales Modell eines Systems (bzw. einer Funktion) bilden, und das dieses die Interaktion mit dem System maßgeblich bestimmt [Lüd04]. Wie diese mentalen Modelle der beteiligten Individuen im Einzelnen aussehen, ist nur schwer zu identifzieren und daher schwer zur Analyse des Problemlösungs- und Entscheidungsverhaltens, bzw. der Möglichkeit ein Schadensereignis zu vermeiden, verwertbar.
Die Kontrollierbarkeit einer vorherrschenden Situation wird in hohem Maße durch das Situationsbewußtsein (engl. situational awareness) der beteiligten Individuen beeinflusst. So zeigen nach [VH06, VGBR10] verschiedene Untersuchungen, dass mit steigender Automatisierung der Anteil von sicherheitskritischen Aktionen pro Bediener und Zeiteinheit ansteigt, die steigende Automatisierung tendenziell die Routine bei seltenen Aktionen reduziert und somit das Situationsbewußtsein abnehmen kann. So besteht beispielsweise die Gefahr, dass ein Fahrer seine Überwachungsaufgabe (z.B. Beobachtung aktuelles Verkehrsgeschehen) vernachlässigt (out-of-the-loop-Effekt), wenn er davon ausgeht, dass diese in ausreichender Weise vom Fahrzeugsystem (z.B. ACC) übernommen wird [WL09]. Werden nun die Systemgrenzen erreicht (z.B. ein direkt vor dem Ego-Fahrzeug einscherendes Fahrzeug) und der Fahrer ist durch die verminderte Aufmerksamkeit nur schlecht über die Verkehrssituation informiert, so kann dies zu verzögerten Reaktionszeiten [VGBR10] und ggf. einem Unfall führen.
Zudem wird die Fähigkeit eine gefährliche Situation zu kontrollieren und ein Schadensereignis abzuwenden nach [VGBR10, WBLS09] in hohem Maße von der Aufmerksamkeitsverteilung der beteiligten Individuen geprägt. So ist davon auszugehen, dass ein Fahrer, der zu stark entlastet wird – die Entlastung ist hierbei von der jeweiligen bereitgestellten Funktion abhängig [GGS09] – die freiwerdenen Ressourcen möglicherweise in Nebentätigkeiten (z.B. Zieleingabe in Navi etc.) investiert, die mit dem Fahren wenig zu tun haben.
Des Weiteren wird das Verhalten der beteiligten Individuen nach [VH06, ABDM09, Hon10], und damit auch die Möglichkeit eine gefährliche Situation zu kontrollieren, in nicht zu vernachlässigbarem Maße von der jeweils vorherrschenden Fahrsituation (inkl. Umwelteinflüsse, Verkehrsaufkommen etc.) [GGS09] und der subjektiven

Risikowahrnemung (z.B. Zero-Risk-Modell[2], Risikohomöoastase[3]) der beteiligten Individuen beeinflusst [AB09].
Die in den vorherigen Abschnitten zusammengestellten Aspekte und die Tatsache, dass die mentalen Modelle, das Situationsbewußtsein und die Aufmerksamkeitsverteilung in der höchst inhomogenen Gruppe der am Straßenverkehr teilnehmenden Individuen [LM06] in hohem Maße streuen, spiegeln die hohe Komplexität der Modelle wider, welche zu einer aussagekräftigen Analyse der Kontrollierbarkeit erforderlich sind. Dieser Tatsache ist es geschuldet, dass das Themengebiet der Simulation und Analyse von Human Factors den Schwerpunkt von einer Vielzahl von Forschungsprojekten darstellt. [VH06, Lüd04, LL05]

8.2 Diskussion des Objektivierungsgegenstandes

In den vorausgehenden Abschnitten wurden die verschiedenen den ASIL bestimmenden Parameter im Detail erläutert. Hierbei wurde sich zunächst losgelöst von der Frage der modellgestützen Objektivierbarkeit auf die Identifikation der, die Parameter S, E und C wesentlich mitbestimmenden Faktoren, diese sind in Tabelle 8.6 gelistet, beschränkt. Im Folgenden wird die Möglichkeit der Objektivierung der einzelnen Faktoren mit simulationsfähigen Modellen diskutiert.
Aus Tabelle 8.6 ist ersichtlich, dass das *Schadensausmaß*, die *Expositionswahrscheinlichkeit* und die *Kontrollierbarkeit* u.a. vom aktuellen *Fahrzeug(bewegungs)-Zustand* und den vorherrschenden *Umgebungsbedingungen* abhängig sind. Daher können mit der Modellierung dieser beiden das Fahrszenario charakterisierenden Parameter die Grundvoraussetzungen geschaffen werden, einen Beitrag zur Objektivierung der ASIL-Parameter zu leisten.

[2]Menschen handeln so, dass ihr subjektives Risiko null beträgt; dieses Modell basiert auf der individuellen Motivation, die das Fahrerverhalten beeinflusst, und der Adaption an das im Straßenverkehr wahrgenommene Risiko [AB09]

[3]Die Theorie der Risikohomöoastase geht davon aus, dass der Mensch bei einer Reduzierung des objektiven Risikos (z.B. durch geeignete technische Maßnahmen) sein Verhalten soweit in Richtung „gefährlicher“ verändert, dass die subjektive Schätzung des Risiko wieder die gleiche Distanz zum pesönlich akzeptierten Risiko erhält wie vor der Einführung der Maßnahme [AB09]

		ASIL-beeinflussende Faktoren									
		Fahrzeugausstattung	Insassen-Konstitution	Unfallgegner	Unfalltyp	Umgebungszustand	Fahrzeugzustand	Mentales Modell	Situationsbewußtsein	Aufmerksamkeitsverteilung	Risikowahrnehmung
ASIL-Parameter	Exposure [E]					x	x				
	Severity [S]	x	x	x	x	x	x				
	Controllability [C]					x	x	x	x	x	x

Abbildung 8.6: ASIL-beeinflussende Faktoren

Die *Expositionswahrscheinlichkeit* in einem relevanten Fahrszenario kann auf Basis der Modellierung und Simulation von den *Fahrzeug(bewegungs)-Zustand* und den *Umgebungsbedingungen* abbildenden Netzen sogar vollständig erschlagen werden. Diese Tatsache und die inhärenten subjektiven Einflüsse während eines jeden szenarienspezifischen Schätzvorgangs werden im Folgenden zum Anlass genommen, dem Schätzenden ein Werkzeug an die Hand zu geben, um die *Expositionswahrscheinlichkeit* (ereignis-)datenbasiert objektiv(er) schätzen zu können. Der im Rahmen dieser Arbeit entwickelte Modellansatz ist in Abschnitt 8.3 im Detail beschrieben.
Ein ähnliches Werkzeug wäre auch zur Unterstützung bei der Abschätzung des *Schadensausmaßes* und der *Kontrollierbarkeit* wünschenswert. Die Umsetzung stellt sich in diesen Fällen aber aufgrund der Vielfalt der in den Abschnitten 8.1.1 und 8.1.3 beschriebenen, und in Tabelle 8.6 zusammengefassten, die Parameter beeinflussenden Faktoren als erheblich schwieriger dar.
So wird in Abschnitt 8.1.1 gezeigt, dass die das Schadensausmaß beeinflussenden Faktoren sogar teilweise voneinander abhängig sind, was ein extrem hohe Modellkomplexität zur Folge hätte. Hierin liegt die Entscheidung begründet, dass im Rahmen der vorliegenden Arbeit vom Versuch einer modellbasierten Objektivierung des Parameters *Schadensausmaß* abgesehen wird.
Gleiches gilt für die *Kontrollierbarkeit*. Allerdings ist hierfür, neben den in Abschnitt 8.1.3 beschriebenen die Komplexität in hohem Maße beeinflussenden Faktoren, insbesondere der Gedanke der Entwicklung einer funktionsunabhängigen Methode ausschlaggebend. Diese Funktionsunabhängigkeit ist für die Kontrollierbarkeit aus nachstehenden Gründen nicht gegeben. Sind beispielsweise mehrere Assistenzfunktionen in einem Fahrzeug realisiert, wird dem Fahrer abhängig vom zur Verfügung stehen-

den Funktionsumfang (z.B. ACC, LKS etc.) bereits bei der Nutzung eines einzigen Fahrzeuges die Adaption an verschiedene Bedienphilosophien abverlangt [GGS09]. Die gleiche Kombination von Assistenzsystemen in einem Fahrzeug eines anderen Herstellers wird die Kontrollierbarkeit ein und desselben Fahrszenarios noch weiter beeinflussen. Es ist also nachvollziehbar, dass die Entstehung eines Unfalls aufgrund verminderter Kontrollierbarkeit aus theoretischer Sicht immer wahrscheinlicher wird, wenn die Anforderungen der Verkehrssituation die Leistungsmöglichkeiten des Fahrers, welche z.B. durch abweichende Bedienphilosophien verschiedener Fahrerassistenzfunktionen negativ beeinflusst werden, übersteigen [WW09].

8.3 Modellbildung – Expositionswahrscheinlichkeit

Im vorhergehenden Abschnitt (Abschnitt 8.1) wurde die grundsätzliche Möglichkeit einer evidenten Modellierung zur Bestimmung der Parameter S, E und C im Detail diskutiert. Hieraus resultiert die Entscheidung, sich im Rahmen der vorliegenden Arbeit auf die modellbasierte Objektivierung des Faktors E zu beschränken. Hierfür wird im Folgenden ein zielführender Modellbildungs-Ansatz beschrieben.
In Abschnitt 4.1 sind die verschiedenen an die *EmMORI-Technik* gestellten Anforderungen im Detail erläutert. Viele dieser Anforderungen lassen sich analog auf den *EmMORI-Modellbildungs-Ansatz* übertragen.
So impliziert die Anforderung, mittels der Methode reproduzierbare Ergebnisse zu erzielen, die Modellierung von simulations- und analysefähigen Modellen (z.B. für Deadlocks).
Des Weiteren müssen die Modelle für die verschiedensten Akteure (Entwickler, Gutachter etc.) nachvollziehbar sein. Hierin liegt die Forderung begründet ein gewisses Maß an Modell-Übersichtlichkeit (z.B. durch Hierachisierung) anzustreben.
Um den Modellbildungs-Ansatz effektiv nutzen zu können bedarf es der Möglichkeit die Modelle ohne allzu großen Aufwand zu adaptieren bzw. aktualisieren und wenn möglich auch zur Lösung neuer Problemstellungen wiederzuverwerten. Insbesondere die Anforderung der Adaptionsmöglichkeit verdeutlicht, dass eine modulare Modellstruktur unabdingbar ist.
Zudem sollte der Modellbildungs-Ansatz ein ausgeglichenes Verhältnis zwischen dem Aufwand der Abbildung eines Ausschnittes der Realität (vgl. AMMIT in Kapitel 4) und der Aussagekraft der Simulations-Ergebnisse aufweisen.

Darüber hinaus sollte der Ansatz der Modellbildung so gewählt sein, dass die Modelle unter Verwendung einer validen Datenbasis (z.B. Statistiken) oder aber basierend auf einfacheren Schätzaufgaben als der Gesamtschätzung parametriert werden können.
In Anlehnung an [Hör04] (vgl. Abschnitt 8.1.2) werden die verschiedenen Merkmale (Umgebungs- und Fahrzeugzustand) mit ihren unterschiedlichen Merkmalsausprägungen in generischen Modulen (Umgebungs-/Fahrzeugzustands-Modul) modelliert, welche sich im Folgenden nur noch in der Parametrierung unterscheiden.
Diese Module werden zu Zustandsmodellen kombiniert, welche anschließend zu Fahrszenarien verkettet werden.
Korrespondierend mit [Hör04] entspricht dieses Fahrszenario dem (Funktions-)Kontext, da die jeweils zu analysierende Funktion in diesem, die Realität abbildenden, Kontext eingesetzt wird.
Wie in Abschnitt 8.1.2 beschrieben, sind zur Bestimmung der Expositionswahrscheinlichkeit in einem Fahrszenario verschiedene Umgebungsbedingungen, unterschiedliche Fahrzeugzustände und deren mögliche Kombinationen zu modellieren.
Das zugehörige Modellbildungs-Konzept wird in den nachstehenden Abschnitten an einem einfachen Beispiel erläutert und auf mathematische Korrektheit überprüft, bevor es in Kapitel 9 auf eine praxisnahe Problemstellung angewendet wird.

8.3.1 Umgebungszustand

Der Umgebungszustand als Verknüpfung der Umstände bzw. Randbedingungen, die bestimmend auf das Fahrer- und Fahrzeugverhalten einwirken, wird von einer Vielzahl (theoretisch unendlich großen Anzahl) von Merkmalen beeinflusst.
Sämtliche Merkmale können in verschiedensten, sich kontinuierlich verändernden Ausprägungen vorherrschen.
Abbbildung 8.7 zeigt exemplarisch, wie im Modell zwei unterschiedliche die Situation bestimmende Merkmale (Merkmals-Module I + II (Plätze)) über zeitlose Entscheidungsstrukturen (gewichtete Transitionen) zu einer Fahrsituation (z.B. I-A-II-X) kombiniert werden können. Merkmals-Modul I (z.B. Verkehrsdichte) weist drei (z.B. freie Fahrt, zähfließender Verkehr, Stau) und Merkmals-Modul II (z.B. Sichtbedingungen) zwei (z.B. gute Sicht, schlechte Sicht) unterschiedliche Merkmalsausprägungen auf.

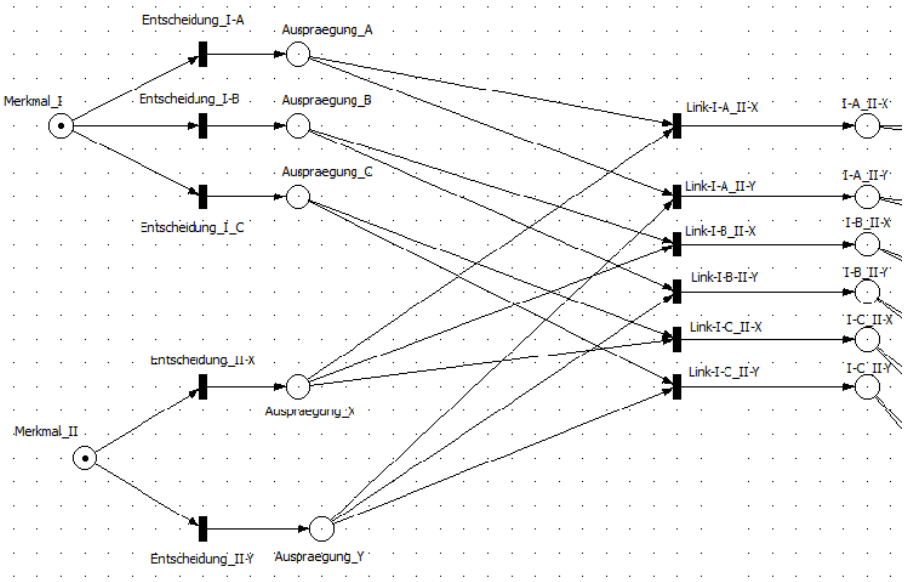


Abbildung 8.7: Umgebungszustand (Situation) – Einfaches Beispiel

Aufgrund der Koexistenz von jeweils genau einer Merkmalsausprägung von Merkmal I und einer von Merkmal II ergibt sich ein „Situationsraum“ von $2 * 3 = 6$ verschiedenen Umgebungs-Situationen (z.B. freie Fahrt – schlechte Sicht).
Sowohl die Anzahl der Merkmals-Module als auch die Anzahl der Merkmalsausprägungen kann theoretisch beliebig angepasst werden, um einen zur Beantwortung der jeweiligen Fragestellung geeigneten Fahrsituations-Raum (z.B. auch „nasse Fahrbahn“ ($\rightarrow$ sehr häufige Situation) , „stehende Objekte (Kiste) auf der Fahrbahn“ ($\rightarrow$ sehr seltene Situation) oder eine Kombination aus beidem) aufzuspannen.

8.3.2 Fahrzeugzustände

Abhängig von der jeweiligen Situation (z.B. werden in der Regel bei schlechter Sicht und hoher Verkehrsdichte keine hohen Geschwindigkeiten gefahren), kann ein Fahrzeug unterschiedlichste Bewegungs- oder Betriebszustände (Plätze) einnehmen. Im Falle des in Abbildung 8.8 dargestellten Beispiels wird zu Anschauungszwecken lediglich unterschieden, mit welcher Wahrscheinlichkeit (hinterlegt in zeitlosen gewichteten Transitionen) sich ein in Betrieb befindliches Fahrzeug im Zustand „Fahrzeug steht“ oder „Fahrzeug fährt“ befindet. Auch hier kann theoretisch eine unendlich große Anzahl von unterschiedlichen Fahrzeugzustands-Modulen modelliert werden

(z.B. „Fahrzeug fährt mit 79 km/h“, „Fahrzeug fährt mit 79,5 km/h“ etc.).

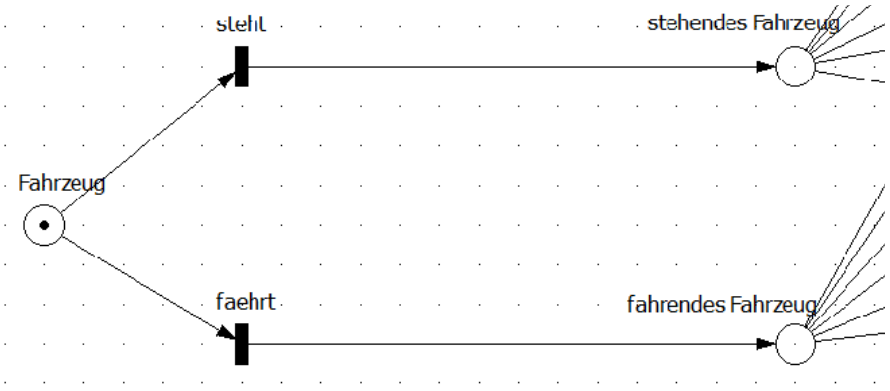


Abbildung 8.8: Fahrzeugzustand – Beispiel

8.3.3 Fahrszenarien als Kombination von Fahrsituationen und Fahrzeugzuständen

Abbildung 8.9 zeigt die Verknüpfung der in den vorherigen Unterabschnitten exemplarisch dargestellten Fahrsituationen und Fahrzeugzuständen zu Fahrszenarien. Aus der Kombinatorik ergeben sich für das Beispiel $6 * 2 = 12$ unterschiedliche Fahrszenarien, deren Eintrittswahrscheinlichkeit bei vorhandener Datenbasis (s. Abschnitt 8.4) durch Simulation und Analyse (s. Abschnitt 8.5) des entwickelten Modells bestimmt werden kann. Zudem ist exemplarische eine Resetter-Transition dargestellt, welche das Gesamtnetz in den Intialzustand überführt.

An dieser Stelle soll kurz auf die Verwandschaft des EmMORI-Modellbildungs-Ansatzes mit der Ereignisbaumstruktur (vgl. Abschnitt 3.1.3) hingewiesen werden. So wird in den Abbildungen 8.7 und 8.8 jeweils von einem Initialzustand ausgegangen und über Entscheidungsstrukturen zwischen alternativen Pfaden ausgewählt. In jedem Zweig bzw. jeder Transition ist dabei eine Wahrscheinlichkeit hinterlegt, die als Zahlenwert für jeden Zweig multipliziert die Wahrscheinlichkeit des Gesamtpfades ergibt.

Der Vorteil des EmMORI-Modellbildungs-Ansatzes gegenüber Ereignisbäumen ist, dass mit ihm sowohl deterministisches als auch stochastisches Verhalten abgebildet werden kann. Herkömmliche Ereignisbäume stoßen bei der Abbildung von stochastischen Verhalten an ihre Grenzen.

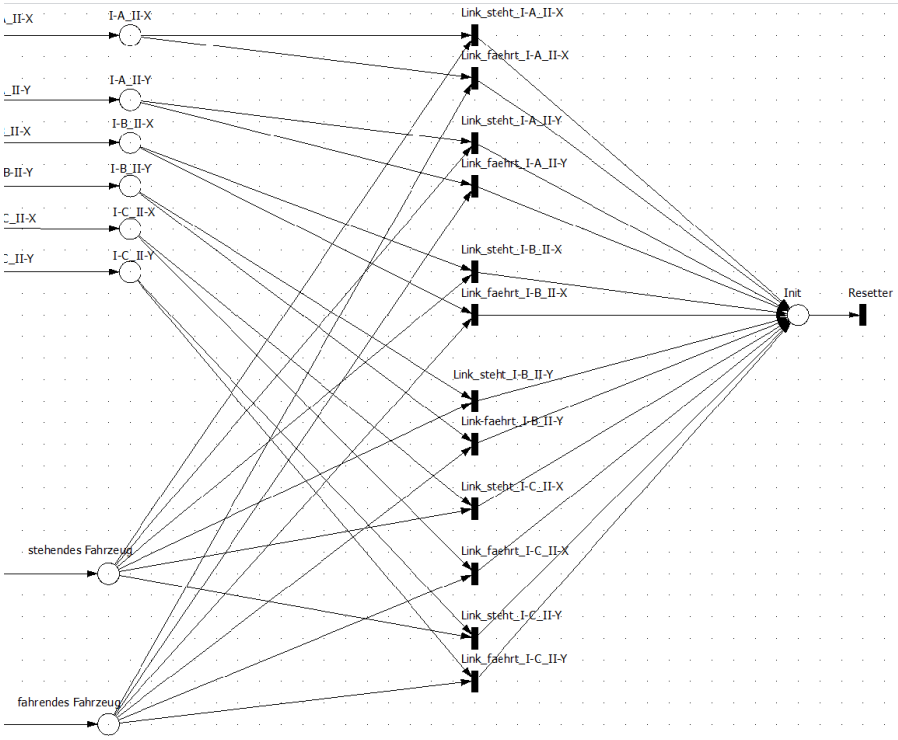


Abbildung 8.9: Fahrszenario – Beispiel

8.4 Modellparametrierung und Datenerhebung

Ist ein die funktionsrelevanten Szenarien abbildendes Modell erstellt, gilt es dieses bzw. dessen Transitionen geeignet zu parametrieren (Abschnitt 8.4.1). Hierzu potenziell zur Verfügung stehende Datenquellen werden in Abschnitt 8.4.2 diskutiert.

8.4.1 Modellparametrierung

Das im Rahmen der EmMORI-Methode genutzte π-Tool bietet die Möglichkeit das Schaltverhalten jeder einzelnen Transition unabhängig zu parametrieren. Hierzu wird dem Anwender ein Verteilungseditor zur Verfügung gestellt, welcher verschiedene Verteilungsfunktionen (z.B. Exponentialverteilung, Weibull-Verteilung etc.) unterstützt.

Die bis hier beschriebenen Modelle verwenden ausschließlich deterministische Transitionen deren Schaltverhalten bei der Entscheidung zwischen Merkmalsausprägungen durch Gewichtungsfaktoren („weight“) bestimmt wird. Ist die Wichtung einer Merkmalsausprägung 0,6 bedeutet dies, dass diese Transition in 60% der Fälle in denen sie schaltfähig ist, schaltet. Die Summe der Wichtungen der von einer Stelle („Merk-

mal“) geschalteten Transitionen ergibt sich hierbei jeweils zu 1.
Zur Modellierung von sich stochastisch verändernden Merkmalsausprägungen werden im Zuge der vorliegenden Arbeit exemplarisch ausschließlich exponentialverteilte Schaltraten verwendet. Der Übergang vom deterministischen zum stochastischen Modell wird hierbei dadurch realisiert, dass die jeweiligen Wichtungswerte des deterministischen Modells übernommen werden und in Form einer Rate in die exponentiellen Transitionen einfließen.

8.4.2 Datenerhebung

Theoretisch kann zur Parametrierung von Modellen auf eine Vielzahl von potenziellen Datenquellen zurückgegriffen werden. Einige Quellen sind nachstehend gelistet:

- *Sammlung von Felddaten (Studien)*: Theoretisch können die Modell-Parameter mit Hilfe eigens durchgeführter Studien gewonnen werden (siehe z.B. [Bast99, BHKP09]). Diese Studien können jedoch sehr zeitaufwendig und damit kostenintensiv sein [DSS10]. In manchen Fällen sind individuelle Situationen aber auch gar nicht oder nur mit unverhältnismäßig großem Aufwand beobachtbar. In solchen Fällen kann zum Teil auf statistische Aussagen aus der Literatur oder vorhandenen Datenbanken (vgl. nachstehende Punkte) zurückgegriffen werden.

- **öffentliche Literatur- und Datenbankquellen**: Hierunter fallen sämtliche (frei) zugänglichen Literaturquellen oder von verschiedenen Institutionen (z.B. Statistisches Bundesamt, Wetterstationen, GIDAS etc.) zur Verfügung gestellte statistische Daten.
  Die Daten zur Parametrierung des PN-Modelles (vgl. Anhang C) zur Objektivierung der Expositionswahrscheinlichkeit erfolgte basierend auf Informationen der nachfolgend gelisteten öffentlichen Quellen:

  - www.bast.de
  - www.destatis.de
  - www.statistik-hessen.de
  - www.zahlenspiegel.net

- **interne Studien und Felderfahrungen**: In einigen Fällen haben OEMs die Möglichkeit auf sehr spezielle Daten aus eigens erstellten Studien (z.B. Unfallforschung [Sta10, SL09, Prä10]) zurückzugreifen, welche das Fahrverhalten/Fahrprofil wiederspiegeln. Hierbei handelt es sich in der Regel um interne Datenbasen, welche der breiten Öffentlichkeit nicht zur Verfügung stehen.

In der Praxis erweist es sich allerdings häufig als sehr schwierig, evidente Daten aus eigenen Studien, Literaturquellen oder Felderfahrungen anderer einzuholen. In diesem Fall kann der Modellierer selbst Werte schätzen oder sich vorliegender Expertenschätzungen bedienen.
Der Vorteil der EmMORI-Methode liegt insbesondere darin, dass die häufig zur Parametrierung des Modells erforderlichen Schätzungen auf ein einfacheres Niveau herabgesetzt werden, als es die Einschätzung der Eintrittswahrscheinlichkeit einer Szenarien-Kombination darstellt.
So fällt es sowohl dem Laien als auch dem Experten in der Regel schwer, abzuschätzen mit welcher Wahrscheinlichkeit sich ein Fahrzeug bei *Dunkelheit* und *schlechten Sichtbedingungen* mit *hoher Geschwindigkeit* innerhalb einer Ortschaft (*innerorts*) fortbewegt.
Wesentlich einfacher wird es, wenn diese eine sehr komplexe Schätzaufgabe in vier einfache(re) kleine Schätzaufgaben zergliedert wird. Im dargestellten Beispiel sind dann folgende vier feingranulare sich teilweise bedingende Schätzaufgaben zu lösen:

- Mit welcher Wahrscheinlichkeit wird das Fahrzeug bei *Dunkelheit* geführt?
- Mit welcher Wahrscheinlichkeit liegen weitere die *Sicht* negativ beeinflussende Faktoren (z.B. Nebel) vor?
- Wie wahrscheinlich ist es, dass das Fahrzeug innerhalb einer *geschlossenen Ortschaft* geführt wird?
- Mit welcher Wahrscheinlichkeit fährt das Fahrzeug unter den gegebenen Randbedingung mit *hoher Geschwindigkeit*?

Durch diese Zergliederung einer komplexen Schätzaufgabe in vier einfache(re) Schätzaufgaben wird auch nicht der in ISO 26262-3 Absatz 7.4.7 beschriebenen Anforderung widersprochen, keine, auf einer zu detaillierten Zergliederung der Betriebssituationen basierende, unangemessene Verringerung der ASIL-Einstufung zu fördern.

Dies wird dadurch sichergestellt, dass zwar die das Fahrszenario charakterisierenden Merkmale einzeln und granular abeschätzt werden, bei der Auswertung aber die für die betrachtete Funktion relevanten Szenarienwahrscheinlichkeiten wieder kumuliert werden (vgl. Abschnitt 8.5.3).

> „..., it shall be ensured that the chosen level of detail of the list of operational situations does not lead to an inappropriate lowering of the ASIL of the corresponding safety goals.“ [ISO DIS 26262-3 7.4.7]

In vielen Fällen wird der ein Modell paramterierende Risikoanalyst nicht nur der Problematik gegenüberstehen über keine valide Datenbasis verfügen zu können. Er wird vielmehr häufig auch mit der Herausforderung konfrontiert, dass sich das zeitliche Verhalten realer Situationen nicht durch deterministische Zeitbewertungen modellieren lässt. Wenn dem so ist, kann jedoch häufig auf Basis zuvor gemachter Beobachtungen (z.B. Niederschlagsstatistiken (vgl. Abb. 8.10 oben)) auf Häufigkeitsverteilungen geschlossen werden.

Diese Verteilung ist in den wenigsten Fällen konstant, sondern vielmehr stochastischen Einflüssen unterworfen. Um dieser Tatsache modelltechnisch begegnen zu können, wurden in Abschnitt 4.3.2 stochastische Petrinetze als Beschreibungsmittel der Wahl identifiziert, welche es ermöglichen den einzelnen Transitionen Verteilungsfunktionen (z.B. Exponential-Verteilung) zu hinterlegen.

8.5 Simulations- und Analyse-Ansatz

In den Abschnitten 8.3 und 8.4 ist der Modellbildungs-Ansatz, die Vorgehensweise zur Datenerhebung und die Modellparametrierung dargestellt.
Bevor auf die Simulation und die Analyse der parametrierten Modelle eingegangen wird, werden zunächst einige Grundlagen zur *Simulation* und zur *Analyse* erläutert.

8.5.1 Auswahl eines geeigneten Simulationsverfahrens

Simulationsverfahren kommen einerseits sehr häufig dann zur Anwendung, wenn analytische Methoden an ihre Grenzen stoßen [Mey00]. Diese Grenzen werden in der Regel erreicht, wenn ein gewisses Maß an Systemkomplexität überschritten wird und/oder stochastisches Verhalten analysiert werden soll [MSS09]. Auf der anderen

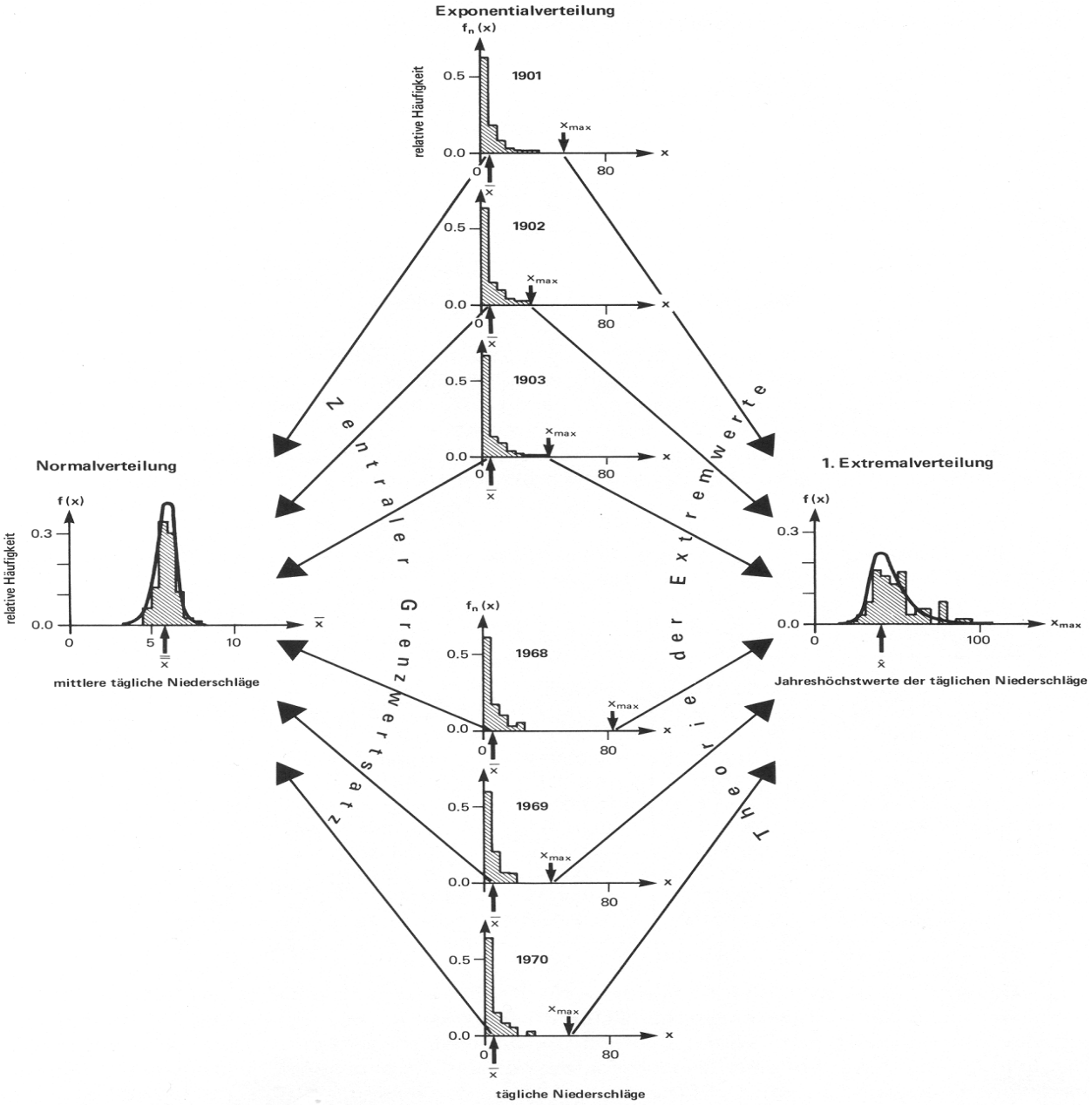


Abbildung 8.10: Niederschlag in Verteilungsfunktionen [Gei91]

Seite wird häufig dann simuliert, wenn das Experimentieren am realen Prozess zu kostenintensiv (z.B. Kraftwerk) oder unvertretbar (z.B. Mensch) ist oder die interessierenden Ereignisse sehr selten sind.

Gerade mit dem Fokus auf den zuletzt genannten Punkt soll die Simulation auch im Rahmen der für die Bestimmung der Expositionswahrscheinlichkeit erforderlichen Analyse von Situationsveränderungen gewinnbringend eingesetzt werden. Der

Vorteil der Simulation liegt hierbei in der Möglichkeit, dass „per Mausklick“ die Eintrittswahrscheinlichkeit verschiedener Umgebungsbedingungen variiert und deren Auswirkung auf den resultierenden ASIL in einem Bruchteil der Echtzeit analysiert werden kann.
In der Literatur (siehe z.B. [AG07, Ste94a]) wird meist zwischen *aufzeichnungsgesteuerter*, *stochastischer* und *deterministischer* Simulation unterschieden. Im Folgenden werden die wichtigsten, die verschiedenen Verfahren charakterisierenden Eigenschaften kurz dargestellt.
Die *aufzeichnungsgesteuerte* bzw. *historische Simulation* geht davon aus, dass alle einen Sachverhalt beeinflussenden Faktoren aus der Vergangenheit auch in Zukunft in gleicher Weise wirken. Sie verzichtet auf eine analytische Untersuchung der Faktoren und stützt sich stattdessen ausschließlich auf in der Vergangenheit gemessene Daten.
Von *deterministischer Simulation* spricht man, wenn alle Daten und Entscheidungsregeln, die in das zu simulierende Modell eingehen, als bekannt angesehen werden. Das deterministische Simulationsmodell bildet die Wirklichkeit unter Ausschluss stochastischer Einflüsse (z.B. werden Wirkungsbeziehungen zwischen Systemelementen oder Umwelteinwirkungen ausgeschlossen (vgl. [RH09])) ab. Alle Parameter werden als fixe Werte angenommen, so dass sich der Modellzustand bei gegebenen Anfangsbedingungen für jeden beliebigen Zeitpunkt eindeutig voraussagen lässt.
Die Annahme, daß ein deterministisches Simulationsmodell vorliegt, ist in vielen Fällen, so auch im Falle der hier zu simulierenden Veränderung von Fahrszenarien beeinflussenden Merkmalen, nicht realistisch, da nur selten eindeutige Aussagen über alle Zusammenhänge (z.B. sich verändernde Sichtbedingungen) eines komplexen Problems gemacht werden können.
Gleichermaßen wird davon ausgegangen, dass das vorliegende Modell aufgrund fehlender Datenaufzeichnungen keineswegs ausschließlich mit historischen Daten befüllt werden kann. Hierin begründet liegt die Entscheidung im Zuge des EmMORI-Ansatzes auf die nachstehend erläuterte *stochastische Simulation* zurückzugreifen.
Unter *stochastischer Simulation* versteht man die Simulation von stochastischen Modellen. Diese beinhalten Elemente, deren Eigenschaften und Relationen vom Zufall abhängig sind. Die Wahrscheinlichkeit des Auftretens eines zufälligen Ereignisses lässt sich hierbei nach seinen Verteilungsgesetzen errechnen. Diese Verteilungsgesetze sind dem Anwender in der Regel nicht von vorneherein bekannt, weswegen eine

empirische Erhebung durchgeführt werden müsste, von der auf eine entsprechendes Verteilungsgesetz geschlossen werden kann. Eine solche Erhebung (z.B. Veränderung von Umgebungseinflüssen, Fahrverhalten etc.) ist in der Regel sehr zeitintensiv und daher mit hohen Kosten verbunden. Zur Lösung dieses Problemes werden Monte-Carlo-Methoden herangezogen, um mit möglichst geringem Aufwand eine möglichst große Stichprobe zu erhalten, welche dem Verteilungsgesetz gehorcht.
Monte-Carlo-Methoden liefern spezielle Verfahren, um komplexe stochastische Problemstellungen zu simulieren, wobei mit Hilfe von künstlich generierten Zufallszahlen bzw. sehr häufig durchgeführten Zufallsexperimenten zufällige Stichproben erzeugt werden, die dem gewünschten Verteilungsgesetz genügen. Dabei können die zu lösenden Probleme selbst zufälliger Natur sein, oder es können deterministische Probleme behandelt werden, für die ein adäquates stochastisches Modell entworfen wird [Beu07]. Die Generierung von Zufallszahlen ist der wesentliche Unterschied zum oben beschriebenen Ansatz der historischen Simulation [RH09].
Für die Anwendung der Monte-Carlo-Simulation kommen nach [RH09] insbesondere Problemstellungen in Betracht in denen komplexe Prozesse nachgebildet werden sollen, die nicht direkt analysiert werden können (z.B. Witterungsbedingungen, Klima der Erde, Aktienkurse etc.).
Da die angestrebte Analyse der Expositionswahrscheinlichkeit in kritischen Fahrszenarien in der Realität keineswegs ausschließlich von sich deterministisch verändernden Parametern abhängt, sondern zu großen Teilen auch stochastischen Einflüssen unterliegt, wird sich im Rahmen dieser Arbeit der Monte-Carlo-Simulation bedient. Sie kann, wie [Slo06, Tro08, MSS09] zeigen, zweckmäßig zur Simulation von stochastischen Petrinetz-Modellen (s. Abschnitt 4.3) herangezogen werden.

8.5.2 Auswahl eines geeigneten Modell-Analyse-Ansatzes

Das grundlegende Ziel einer Modell-Analyse, also einer systematischen Untersuchung des Modells, ist es, für ein explizit beschriebenes Modell das damit implizit gegebene Modellverhalten zu untersuchen.
Da jede Modellierung auf die Abstraktion eines Ausschnitts der realen Welt abzielt, kann die Modellanalyse im Hinblick auf zwei unterschiedliche Zielsetzungen durchgeführt werden.
Dies ist zum einen die Modellverifikation, in der das Modell auf das korrekte Verhalten im Rahmen der gewählten Abstraktionsstufe geprüft wird. Zum anderen wird

von der Modellvalidation gesprochen, wenn das erzielte Modellverhalten mit dem Verhalten des abgebildeten Ausschnittes der Realwelt verglichen wird.
Der Fokus der vorliegenden Arbeit liegt diesbezüglich auf der Validation des Modells bzw. der Methode. Hierzu werden die Ergebnisse der Modell-Analyse gegen die auf Basis der ISO 26262 durchgeführten Schätzungen geprüft (vgl. Abschnitt 7.2.1).
Eine Verifikation der Modelle kann aufgrund der Tatsache, dass analytische Methoden, gegen deren Ergebnisse geprüft werden könnte, aufgrund der Komplexität sich stochastisch verändernder Umgebungseinflüsse an die oben genannten Grenzen stoßen, nicht vollständig erbracht werden.
Grundsätzlich können zur Untersuchung des Modell-Verhaltens zwei Analysemethoden angewendet werden, die *transiente* und die *stationäre* Analyse.
Liegt beim vorgegebenen Modell das Interesse darin, eine Aussage darüber zu treffen, welchen Zustand $N(t)$ ein System bei gegebenem Anfangszustand zu einem bestimmten Zeitpunkt t eingenommen hat, so ist die transiente Analyse zielführend. Die verwendete Bezeichnung „transient“ erklärt hierbei, dass das beschriebene gegebenenfalls sehr komplizierte Modell-Verhalten unter Umständen nur für eine Übergangszeit vorliegt.
Stochastische Prozesse, welche sich nach hinreichend langer Zeit ($t \to \infty$) zunehmend einem stationären Zustand nähern, d.h. ein Verhalten aufzeigen, bei dem die Verteilungen von $N(t)$ unabhängig von t sind und gegen einen Wert konvergieren, bieten die Möglichkeit der *stationären Analyse* [BC09]. Diese Analyse gibt an, wie sich das Modell im eingeschwungenen Zustand („Gleichgewichtsverhalten“) verhält. Dieses Gleichgewichtsverhalten ist für die Wahrscheinlichkeit der Exposition in einem bestimmten Fahrszenario von Interesse, weswegen sich im Zuge der EmMORI-Methode der *stationären Analyse* bedient wird, um quantitative Aussagen treffen zu können. So kann auf Basis der, in den Transitionen hinterlegten, statistisch verteilten und somit die Merkmalausprägung bestimmenden Raten der eingeschwungene Zustand der Expositions-Wahrscheinlichkeit in einem kritischen Fahrszenario bestimmt werden.

8.5.3 Simulation und Analyse am einfachen Beispiel

In Abschnitt 8.3 sind die verschiedenen Modell-Module (Fahrsituation, Fahrzeugzustand und Kombination), mittels welcher sich beliebig abstrakte, aber auch beliebig detaillierte Fahrszenarien abbilden lassen, beschrieben.

Ziel dieses Abschnittes ist es die Anwendung dieser Modelle zur toolgestützten, auf Monte-Carlo-Simulation (vgl. Abschnitt 8.5.1) basierenden, Bestimmung der Expositionswahrscheinlichkeit exemplarisch aufzuzeigen.
Wurden potenzielle Fehlfunktionen der zu entwickelnden Funktion bzw. des zu entwickelnden Systems wie in Abschnitt 7.2.1 dargelegt identifiziert, gilt es im Folgenden u.a. die Aufenthaltswahrscheinlichkeit zu bestimmen, mit der sich ein Fahrzeug in einem Szenario befindet, in der die betrachtete Fehlfunktion potenziell gefährlich werden kann.
Im Beispiel werden die (virtuellen) Zustände als kritisch, d.h. im Sinne der Analyse interessierend, angenommen, welche sich aus der Schaltung der Transitionen „Link-faehrt-IB-IIX“ und „Link-faehrt-IA-IIY“ ergeben.
Es wird zudem angenommen, dass die beiden Szenarien in einem einhüllenden, für die betrachtete Fehlfunktion relevanten Fahrszenario zusammengefasst werden können. Die Wahrscheinlichkeit der Exposition im einhüllenden Fahrszenario ergibt sich durch die Summation der einzelnen Pfadwahrscheinlichkeiten, die zu diesem Fahrszenario führen.
Die besagten Zustände selbst werden im Modell nie erreicht, da die an deren Post-Kanten verorteten Transitionen modelltheoretisch gleichermaßen als „Auswerte- bzw. Zähltransitionen“, deren Schalthäufigkeit von Interesse ist, aber auch als „Resetter“ fungieren, welche das Netz nach dem Schalten dieser Transition für den nächsten Simulations-Durchlauf initialisieren.
Für die Transitionen ergeben sich bei gegebenen Parameterwerten (s. Tabelle 8.2) die in Tabelle 8.3 enthaltenen Wahrscheinlichkeiten.

Tabelle 8.2: Fiktive Modell-Parameter (Beispiel)

Transition	**Gewichtung**
Entscheidung-IA	0,3
Entscheidung-IB	0,6
Entscheidung-IC	0,1
Entscheidung-IIX	0,8
Entscheidung-IIY	0,2

Diese entsprechen dem prozentualen Anteil der Gesamt-Betriebszeit (ignition on) des Fahrzeuges, in der sich das Fahrzeug im relevanten Szenario befindet und die Fahrzeuginsassen exponiert sind.

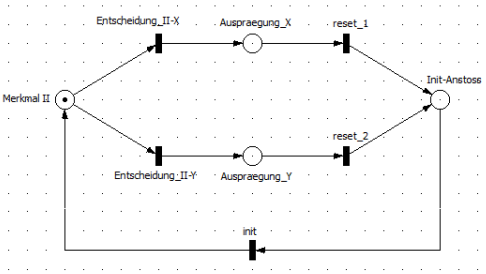
Tabelle 8.3: Einzel-Wahrscheinlichkeiten des Aufenthalts in betreffendem Szenario

Transition	**Wahrscheinlichkeit**
Link-faehrt-IB-IIX	0,054
Link-faehrt-IA-IIY	0,432

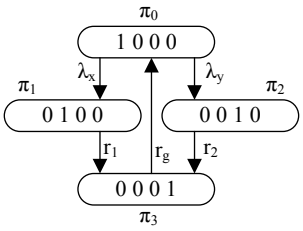
Nachstehender Kasten erläutert exemplarisch die zugrunde liegenden vom Simulations- und Analyse-Werkzeug π-Tool ausgeführten Rechenoperationen.

Exemplarische Berechnung der Zustandswahrscheinlichkeiten

Nachstehende Abbildung zeigt den, die Entscheidung zwischen den Merkmalsausprägungen Ausprägung X und Ausprägung Y des Merkmals II realisierenden Modell-Ausschnitt. Das Modell ist hierbei um eine Initialisierungsschleife erweitert, welche im Fahrszenarien-Modell an anderer Stelle gleichermaßen implementiert ist.



In der folgenden Abbildung ist der zugehörige Erreichbarkeitsgraph für das Entscheidungsverhalten bei gegebener Anfangsmarkierung dargestellt.



Aus dem Erreichbarkeitsgraphen wird die Zustandsübergangsmatrix Q bestimmt:

$$Q = \begin{pmatrix} -\lambda_x - \lambda_y & 0 & 0 & r_g \\ \lambda_x & -r_1 & 0 & 0 \\ \lambda_y & 0 & -r_2 & 0 \\ 0 & r_1 & r_2 & -r_g \end{pmatrix}$$

Mit den Randbedingungen $Q\pi = 0$ und $\pi_0 + \pi_1 + \pi_2 + \pi_3 = 1$ und der Annahme $r_1 = r_2 = r_g = 1$ ergeben sich nach einigen Rechenoperationen nachstehende Lösungen für die stationären Zustandswahrscheinlichkeiten.

$$\pi_0 = \pi_3 = \frac{1}{\frac{1-y}{x} + x + y + 1} \qquad \pi_1 = x\pi_0 \qquad \pi_2 = y\pi_0$$

Mit diesen Gleichungen kann die stationäre Zustandwahrscheinlichkeit des jeweils interessierenden Zustandes (z.B. Ausprägung-x $\rightarrow \pi_1$) berechnet werden.

Unter Verwendung der in Tabelle 8.4 [s. Tab. B2 in ISO DIS 26262-3] angegebenen Wahrscheinlichkeits-Intervalle lässt sich der Parameter der Wahrscheinlichkeit des Aufenthalts (Probability of Exposure) im betreffenden Szenario bestimmen.

Tabelle 8.4: Kategorien von Aufenthaltswahrscheinlichkeiten

Class	**E0**	**E1**	**E2**	**E3**	**E4**
Definition of duration/ probability of exposure	Incredible	Not specified ($\ll$1 %)	<1 % of average operating time	1 - 10 % of average operating time	>10 % of average operating time

Hierzu wird die Summe (vgl. Gleichung 8.1) der Eintrittswahrscheinlichkeiten der einzelnen als relevant eingestuften Szenarien gebildet und gemäß Tabelle 8.4 der Kategorie E4 zugewiesen.

$$P_{Link-faehrt-IB-IIX} + P_{Link-faehrt-IA-IIY} = 0,054 + 0,432 = 0,486 \approx 50\% \quad (8.1)$$

Unter Hinzunahme der auf die herkömmliche Weise nach ISO 26262 bestimmten Parameter *Kontrollierbarkeit* und *Schadensausmaß* kann dann mittels der Risikomatrix (s. Tabelle 7.1) der für die betreffende Funktion erforderliche ASIL bestimmt werden.

8.6 Validation des Ansatzes

Ziel dieses Abschnittes ist es das in den vorhergehenden Abschnitten entwickelte Modellbildungs-Konzept gegen eine anerkannte und im Umfeld der Sicherheits- und Zuverlässigkeitsanalyse weit verbreitete Technik zu validieren. Hierzu wird sich der Technik „Ereignisbaumanalyse“ bedient, welche nach Abschnitt 4.2 die an die entwickelte EmMORI-Methode gestellten Anforderungen zu großen Teilen gleichermaßen erfüllt.
Die Korrektheit der Simulations-Ergebnisse (s. Tabelle 8.3) der Petrinetzmodelle lässt sich, wie in Abbildung 8.11 gezeigt, für das einfache Beispiel unter Verwendung

der Ereignisbaumanalyse nachweisen. Dies gilt allerdings nur, solange ausschließlich von deterministischen Merkmalsunterscheidungen ausgegangen wird.

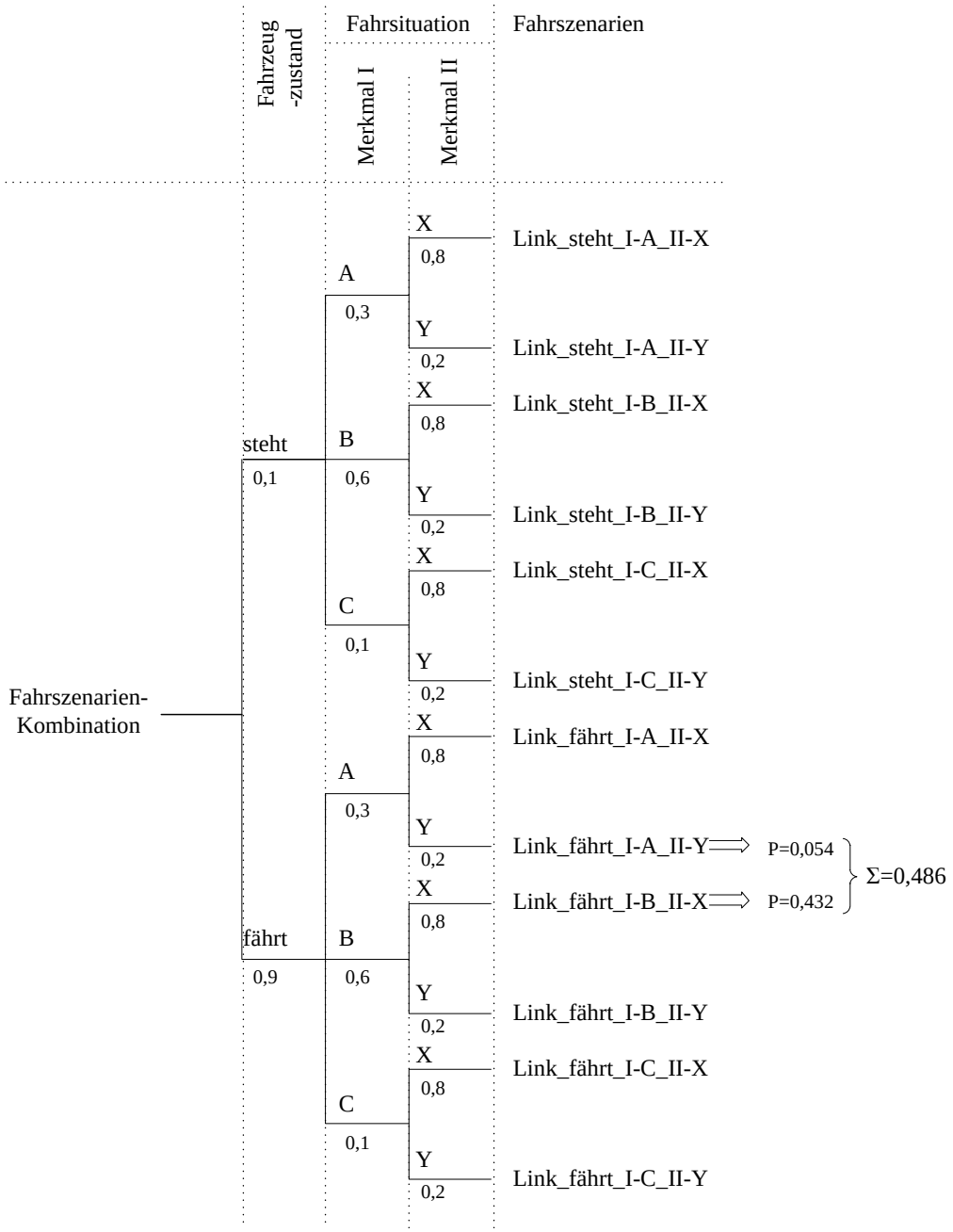


Abbildung 8.11: Ereignisbaumanalyse zur Validation des einfachen Beispiels

Folgen die Parameter stochastischem Verhalten, stößt die Ereignisbaumanalyse aufgrund ihrer Beschränktheit auf deterministische Parameter an ihre Grenzen. Die-

se Einschränkung ist zwar irrelevant für die Validation des Modellierungsansatzes bzw. die Modellstruktur, nicht aber für eine realitätsnähere Abbildung von Fahrszenarien, weswegen Petrinetze zur Modellierung vorzuziehen sind. Ziel ist es die Umgebung und den Fahrzeugzustand mit den zur Verfügung stehenden Ressourcen möglichst dem tatsächlichen Sachverhalt entsprechend abzubilden, um die Wahrscheinlichkeit der Exposition in interessierenden Fahrszenarien objektiv bestimmen zu können. Aus diesem Grund wird sich im Zuge der Modellierung des Anwendungsbeispiels (s. Abschnitt 9.2) von der Annahme distanziert, dass die ein Fahrszenario bestimmenden Merkmale (z.B. Witterungsbedingungen (vgl. Abschnitt 8.5.1)) einem rein deteriministischem Verhalten gehorchen.
Hierzu wird in den die Merkmalsausprägungen bestimmenden Transitionen exemplarisch jeweils eine exponentialverteilte Rate hinterlegt (s. Gleichung 8.2), um stochastisches Verhalten simulieren zu können.

$$P(t) = e^{-rt} \tag{8.2}$$

Unter der Annahme, dass die Merkmalsausprägungen differenzierenden Raten (vgl. Anhang C) konstant sind ($r = const$), hiervon ist auf lange Sicht auszugehen, ergibt sich die in Abbildung 8.12 skizzierte Verteilung der Wahrscheinlichkeit des Vorliegens einer bestimmten Merkmalsausprägung.

Modelltheoretisch ist dies wie folgt zu interpretieren. Da das Gesamtmodell im Rahmen der Monte-Carlo-Simulation nach jeder Schaltung einer Initialisierungs-Transition, also dem Eintreten eines beliebigen Fahrszenarios, initialisiert wird, läuft die Zeit immer wieder von null bis zu einem zufälligen Zeitpunkt $T_{MC,n}$. Der zugehörige y-Wert wird als eine die Merkmalsentscheidung beeinflussende Schaltwahrscheinlichkeit an das Gesamtmodell übergeben, wodurch die Eintrittswahrscheinlichkeit der verschiedenen Fahrszenarien bestimmt wird.

8.7 Zusammenfassung – Modellbildung, Simulations- und Analyse-Ansatz

Die grundlegende Idee dieser Arbeit ist die Objektivierung des Verfahrens zur ASIL-Bestimmung, wie es in ISO 26262 vorgeschlagen wird.
Kapitel 8 stellt das Konzept dar, welches zur Lösung dieses Objektivierungsproblems

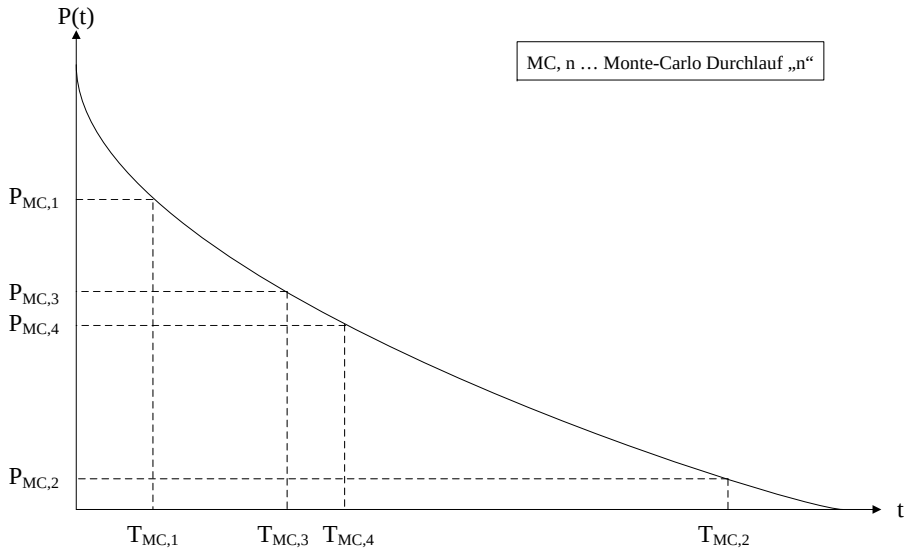


Abbildung 8.12: Verteilungsfunktion der Existenz einer spezifischen Merkmalsausprägung

entwickelt wurde.
Hierzu wird in den Abschnitten 8.1.1, 8.1.2 und 8.1.3 die Objektivierbarkeit der einzelnen den ASIL charakterisierenden Parameter diskutiert.
Auf Basis der erbrachten Argumente wird sich im Rahmen der vorliegenden Arbeit auf die Objektivierung des Faktors *Expositions-Wahrscheinlichkeit (E)* beschränkt. Auf potenzielle Objektivierungsansätze der verbleibenden Faktoren *Kontrollierbarkeit (C)* und *Schadensausmaß (S)* wird kurz in Abschnitt 10.2 eingegangen.
Abschnitt 8.3 beschreibt den eigentlichen Modellbildungsansatz mit seinen einzelnen Modell-Modulen (Fahrsituation und Fahrzeugzustand) und deren Kombination zu Fahrszenarien, deren Eintrittswahrscheinlichkeit für die Abschätzung der Werte des Parameters E von Interesse ist.
Der Schwerpunkt von Abschnitt 8.4 liegt auf der Darlegung potenzieller Datenquellen, z.B. interne/externe Studien, öffentliche Datenbanken, Expertenschätzungen, welche zur Parametrierung des entwickelten Modells genutzt werden können.
In Abschnitt 8.5.1 wird die Monte-Carlo-Simulation als geeignetes Verfahren zur Simulation der in Abschnitt 8.3 dargestellten hierarchischen stochastischen Petrinetz-Modelle bestimmt. Anschließend werden in Abschnitt 8.5.2 die zur Auswahl stehenden, mit der Monte-Carlo-Simulation in Einklang zu bringenden Analyse-Verfahren, die *transiente* Analyse und die *Steady-State*-Analyse, diskutiert. Da im Zuge der

Untersuchung der Expositions-Wahrscheinlichkeit in einem interessierenden Zustand das Modell-Verhalten, bzw. die Schaltwahrscheinlichkeit der Auswerte-Transitionen im eingeschwungenden Zustand von Interesse ist, wird die Steady-State-Analyse als zielführendes Verfahren identiziert.
Die verschiedenen Teilaspekte des Konzeptes *Modellbildung, Datenerhebung* und *Simulation und Analyse* werden an einem einfachen Beispiel aufgezeigt.
In Abschnitt 8.6 werden die mittels Simulation und Analyse der Modelle gewonnen Ergebnisse validiert. Hierzu werden die modelltheoretisch bestimmten Eintrittswahrscheinlichkeiten mit den Ergebnissen einer Ereignisbaum-Analyse (ETA) verglichen und auf numerische Übereinstimmung überprüft.

Kapitel 9

EmMORI-Anwendungsbeispiel

Ziel dieses Kapitels ist es, die entwickelte EmMORI-Methode auf eine praxisnahe Problemstellung zu übertragen, und soweit möglich zu validieren.
Als praxisnahe Problemstellung bietet sich, auch im Hinblick auf die angestrebte Validation, die ASIL-Einstufung der in Abschnitt 7.2 beschriebenen, und nach dem in ISO 26262 vorgeschlagenen Vorgehen eingestuften, Funktion „Abblendlicht“ an.
Bereits in Kapitel 8 wird darauf hingewiesen, dass die EmMORI-Methode als ein konkreter Vorschlag zur modellbasierten Erweiterung der Gefährdungs- und Risikobewertung gemäß ISO 26262 zu sehen ist, welche die ASIL-Einstufung objektivieren kann.
Hierbei ist zu beachten, dass die EmMORI-Methode erst dann sinnvoll angewendet werden kann, wenn die vorhergehenden Teilschritte der Gefährdungsanalyse und Risikobewertung (vgl. Abschnitt 7.2.1) strukturiert abgearbeitet wurden.
Erst im Rahmen der *Bestimmung der Sicherheitsklasse* gilt es die identifzierten Gefährdungen auf potenziell kritische Szenarien abzubilden und zu bewerten. Hierzu werden die Wahrscheinlichkeit der Exposition im Szenario (Faktor E), das potenziell von der Gefährdung ausgehende Schadensausmaß (Faktor S) und die Möglichkeit der Gefährdungsabwehr (Faktor C) bisher nach ISO 26262 auf Basis rein subjektiver Erfahrungswerte abgeschätzt (vgl. Abschnitt 7.2.1).
Mittels der EmMORI-Methode wurde es angestrebt diese Schätzungen modellgestützt zu objektivieren. Allerdings musste im Zuge der Untersuchung der realitätsnahen Abbildbarkeit der die einzelnen Faktoren (s. Abschnitte 8.1.1 bis 8.1.3) beeinflussenden Parameter festgestellt werden, dass die zahlreichen das Schadensausmaß und die Kontrollierbarkeit beeinflussenden Einflussgrößen eine handhabbare Modell-

komplexität übersteigen lassen würde.
Hierin begründet liegt die Entscheidung, dass im Rahmen der vorliegenden Arbeit lediglich die modellgestützte Objektivierung der Expositionswahrscheinlichkeit verfolgt wird.

9.1 Modellbildung der Fahrszenarien

In einem ersten Schritt gilt es ein der betrachteten Funktion gerecht werdendes Modell zu entwickeln, welches die für die Funktion relevanten Szenarien umfasst. Hierzu kann sich genau der in Abschnitt 8.3 beschriebenen generischen Modell-Module bedient werden, welche aus Gründen der Übersichtlichkeit bzw. Nachvollziehbarkeit in eine hierarchisierte Modellstruktur einfließen.
Die Modell-Module mit ihren unterschiedlichen Merkmalsausprägungen werden sowohl zur Abbildung von *Fahrsituationen* als auch zur Modellierung von *Fahrzeugzuständen* hinzugezogen und in einem hierarchischen Modell zu *Fahrszenarien* kombiniert.

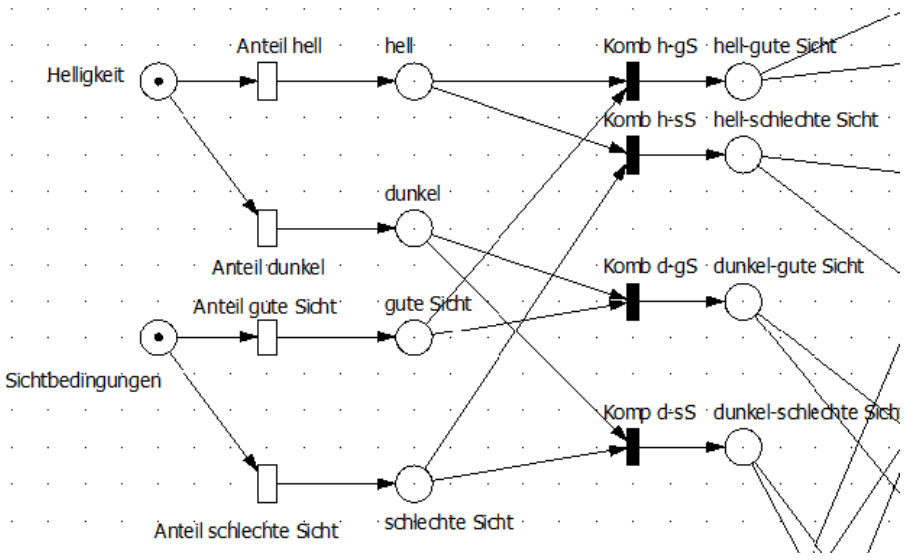


Abbildung 9.1: Fahrsituation - Helligkeit und Sichtbedingungen

Abbildung 9.1 zeigt einen Ausschnitt des die Fahrsituation beschreibenden Modells. Dieser Teilbereich des Modells wird durch die verschiedenen Merkmalsausprägungen der Merkmale *Helligkeit* und *Sichtbedingungen* aufgespannt. Da im Rahmen

dieser methodenorientierten Untersuchung, welche keinen Anspruch auf Vollständigkeit erhebt, nur jeweils zwei Merkmalsausprägungen ($n = 2$, $m = 2$) angenommen werden, ergibt sich ein Situationsraum von vier ($2 * 2 = 4$) unterschiedlichen Helligkeits/Sichtbedingungs-Kombinationen. Für den Fall, dass eine endliche Anzahl von Merkmalsausprägungen zweier Merkmale (n, m) angenommen wird, ergeben sich jeweils $n * m$ Attributs-Kombinationen.
Analog zu den Fahrsituationen lassen sich, wie in Abbildung 9.2 exemplarisch gezeigt, unter Verwendung der in Abschnitt 8.3 dargestellten Modell-Module auch unterschiedlichste Fahrzeugzustände darstellen.

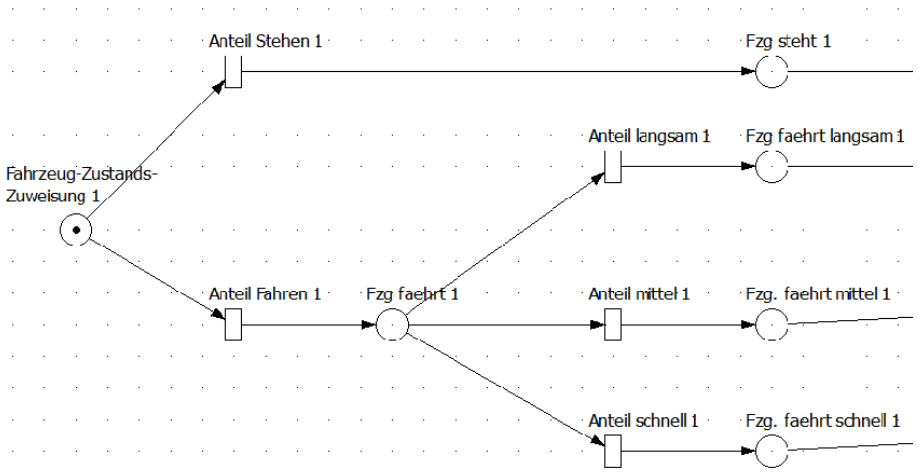


Abbildung 9.2: Fahrzeugzustand - Geschwindigkeitsunterscheidung

Der vorgestellte Ansatz differenziert zwischen verschiedenen Bewegungszuständen (steht/fährt) bzw. Geschwindigkeiten (langsam/mittel/schnell) des Fahrzeuges. Dies vor dem Hintergrund, dass gerade die Geschwindigkeit bzw. die davon abhängige kinetische Energie bei einer Kollision für das Schadensausmaß eines Schadensereignisses mitbestimmend ist.
Durch Kombination der unterschiedlichen Fahrsituationen mit den einzelnen Fahrzeugzuständen lässt sich der gesamte Szenarienraum, in dem sich der Nutzer eines mit der betrachteten Funktion ausgestatteten Fahrzeuges wiederfinden kann, darstellen.
Modelltechnisch wird diese Kombination erreicht, indem jede Fahrsituation in die den Fahrzeugzustand beschreibenden Modelle eingespeist wird (vgl. Abbildung 9.3).

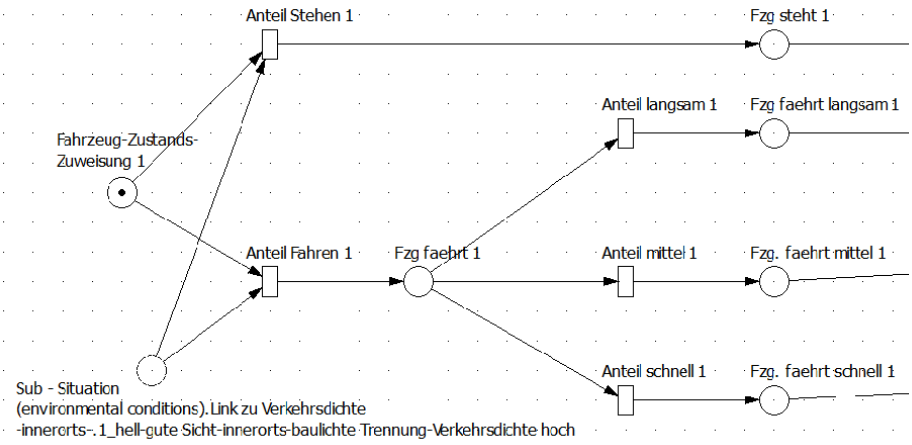


Abbildung 9.3: Einbindung Fahrsituation in Fahrzeugzustand

Im Falle des entwickelten Gesamtmodells (s. Ausschnitte in Abbildung 9.6 und in Anhang B) ergibt sich aus der Kombination der Merkmalsausprägungen der sechs Merkmale ein Szenarienraum von 128 unterschiedlichen Szenarien (vgl. Abbildung 9.4).

Merkmalsbereich	Umgebung / Fahrsituation					Fahrzeugzustand
Merkmal	Helligkeit	Sichtbedingungen	Ort	bauliche Trennung	Verkehrsdichte	Bewegungszustand
Kombination der Merkmalsausprägungen	hell dunkel	gut schlecht …	innerorts außerorts …	ja nein …	… hoch niedrig	… steht — Sz_{abc} fährt langsam — Sz_{efg} fährt mittelschnell — Sz_{hij} fährt schnell — Sz_{xyz}
Anzahl der Szenarien	2	x 2	x 2	x 2	x 2	x 4 = 128

Abbildung 9.4: Ereignisbaumbasierte Herleitung des Szenarienraums

Dieser Szenarienraum bleibt bei einer gegebenen Anzahl von Merkmalen und Merkmalsausprägungen konstant, da davon ausgegangen wird, dass sämtliche Merkmalsausprägungen mit einer Wahrscheinlichkeit von P>0 auftreten, und daher bei der Verfolgung eines speziellen ein Szenario generierenden Pfades immer die gleiche Anzahl von Merkmalsausprägungen kombiniert wird.
Hierbei wäre durch die Festlegung einer Grenz-Wahrscheinlichkeit, welche die Weiterverfolgung des jeweiligen betroffenen Pfades unterbindet, theoretisch eine Reduktion der zu untersuchenden Szenarien, und dadurch der benötigten Rechenkapazität,

möglich. Dieser Ansatz wird jedoch hier nicht weiter verfolgt, da es vielmehr das Ziel ist sämtliche relevanten und potenziell in der Realität auftretenden Szenarien abzubilden, um bei der Szenarienanalyse ein hohes Maß an Vollständigkeit zu erreichen. Aufgrund dieses expliziten Unterlassens der Definition und Implementierung von die Modellkomplexität reduzierenden Grenzwahrscheinlichkeiten, und unter der Annahme der statistischen Unabhängigkeit der verschiedenen Merkmale, hat die Reihenfolge der Merkmale bei der Modellierung der Fahrsitationen/-szenarien keinen Einfluss auf die resultierenden Wahrscheinlichkeiten (vgl. Abbildung 9.5).

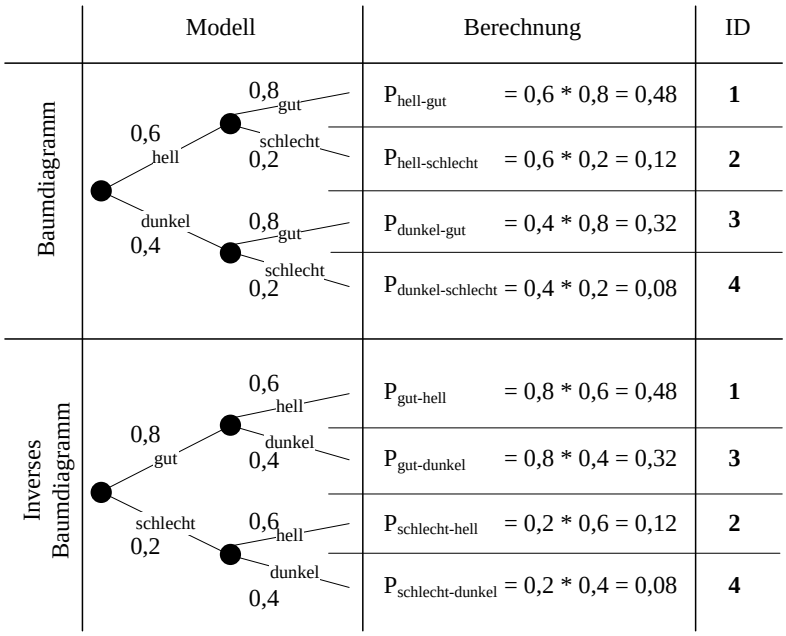


Abbildung 9.5: Reihenfolge und statistische Unabhängigkeit

Die Vertauschung der Merkmale im Modell führt zwar zu einem inversen Modell. Die Wahrscheinlichkeiten der Ausbildung der unterschiedlichen Situationen stimmen jedoch bis auf deren Verortung (s. ID) im Modell für beide Modell-Varianten überein.

Sowohl das die Fahrsituation als auch das den Fahrzeugzustand abbildende Modell kann theoretisch je nach bearbeiteter Fragestellung bzw. einzustufender Funktion beliebig verfeinert oder angepasst werden. Die hier vorgestellte Modellstruktur ist keineswegs bindend, umfasst aber die für die Modellierung der Funktion „Abblendlicht“ relevanten, die Szenarien charakterisierenden, Merkmale.

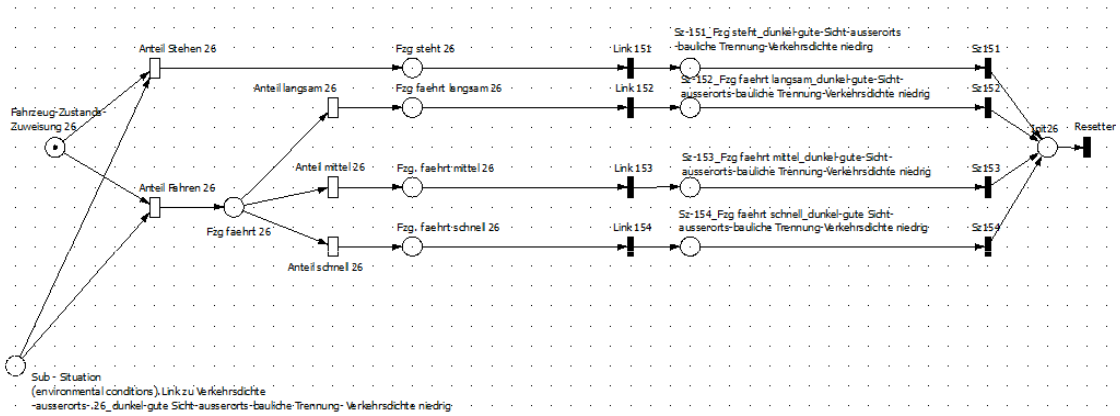


Abbildung 9.6: Generierte Fahrszenarien (Auszug)

Die Merkmalsrelevanz für die Funktion „Abblendlicht“ kann wie folgt argumentiert werden:

- Fahrsituation:
  - **Helligkeit**: Erst bei Dunkelheit ist die Funktion „Abblendlicht“ zwingend erforderlich. Dennoch soll hier nicht versäumt werden zu erwähnen, dass verschiedene Studien aufzeigen, dass auch das Tagfahrlicht einen erheblichen Einfluss auf die Verkehrssicherheit hat [SEGT05, EU08].
  - **Sichtbedingungen**: Sowohl das „Sehen“ als auch das „Gesehenwerden“ werden bei schlechten Sichtbedingungen durch das Abblendlicht positiv beeinflusst.
  - **Ort**: Zu großen Teilen kann davon ausgegangen werden, dass innerstädtische Straßen nachts beleuchtet sind, weswegen ein Versagen der Funktion „Abblendlicht“ dort weniger kritisch ist als außerorts. Die Kritikalität des Versagens der Funktion „Abblendlicht“ ist demnach abhängig vom Ort.
  - **bauliche Trennung**: Im Falle des Vorhandenseins einer baulichen Trennung zwischen den Fahrspuren kann davon ausgegangen werden, dass Unfälle, welche sich auf eine Fehlfunktion des Lichtes zurückführen lassen, mit großer Wahrscheinlichkeit ein geringeres Schadenspotenzial bergen als auf einer Straße ohne bauliche Trennung, da Frontalzusammenstöße mit einem anderen Fahrzeug (so gut wie) ausgeschlossen sind.
  - **Verkehrsdichte**: Ist die Verkehrsdichte hoch, so kann ein Fahrzeug mit defektem „Abblendlicht“ in einer Kolonne „mitschwimmen“. Sind dage-

gen keine weiteren Fahrzeuge vorhanden, an denen sich der Führer des Fahrzeuges orientieren kann, so wird es mit größerer Wahrscheinlichkeit zu einem Unfall kommen.

- Fahrzeugzustand:
  - **Geschwindigkeit**: Die (Relativ-)Geschwindigkeit hat erheblichen Einfluss auf das Unfallgeschehen und das potenzielle resultierende Schadensausmaß.

Jedes der gelisteten Merkmale wird in einem Merkmals-Modell (analog der beiden Module für *Helligkeit* und *Sichtbedingungen* in Abbildung 9.1) abgebildet. Die unterschiedlichen Ausprägungen der die Fahrsituation charakterisierenden Merkmals-Modelle werden dann modelltechnisch kausal mit den verschiedenen den Fahrzeugzustand bestimmenden Merkmalen (z.B. Geschwindigkeit) verknüpft und auf Basis logischer Überlegungen parametrisiert (z.B. schlechte Sichtbedingungen - hohe Verkehrsdichte → hohe Geschwindigkeit unwahrscheinlich, gute Sichtbedingungen - niedrige Verkehrsdichte → hohe Geschwindigkeit wahrscheinlich).

9.2 Modellparametrierung, -simulation und -analyse

Im vorhergehenden Abschnitt 9.1 wurde das zur Objektivierung der Expositions-Wahrscheinlichkeit in einem abblendlicht-relevanten Szenario entwickelt.
Dieses gilt es im folgenden geeignet zu parametrisieren, zu simulieren und die Ergebnisse der Simulation zu analysieren.
Zur Parametrisierung kann sich theoretisch der in Abschnitt 8.4.2 näher erläuterten Datenquellen bedient werden.
Ein Parametrisierungs-Vorschlag des Gesamt-Modells ist in Anhang C gegeben. Die dort hinterlegten Werte zur Quantifizierung der Wahrscheinlichkeit des Auftretens der Umgebungsbedingungen und der Fahrzeugzstände basieren größtenteils auf feingranularen Schätzungen (vgl. Abschnitt 8.4.2) und öffentlich zugänglichen Quellen.
Zur Simulation der entwickelten Modelle wird sich der in Abschnitt 8.5.1 als sinnvoll einsetzbar identifizierten Monte-Carlo-Methode bedient. Mit Hilfe der stationären Modell-Analyse (vlg. Abschnitt 8.5.2) wird dann die Wahrscheinlichkeit der Exposition in einem abblendlicht-relevanten Szenario bestimmt. Sowohl Simulation als auch Analyse werden hierbei mit dem in Abschnitt 4.4 näher erläuterten π-Tool

durchgeführt.
In Abschnitt 9.3 werden die erzielten Ergebnisse der Analyse des Gesamtmodells zum Anwendungsbeispiel „Abblendlicht“ und deren Validierung diskutiert.

9.3 Ergebnis-Analyse und -Plausibilisierung

Die Modell-Analyse lässt aufgrund des gezielt generisch angelegten, also funktionsunabhängigen Ansatzes nicht direkt auf das angestrebte Ergebnis schließen. Die gesuchte Expositions-Wahrscheinlichkeit im jeweiligen Szenario ist vielmehr problemorientiert aus den Ergebnissen der Modell-Analyse herauszufiltrieren.
Dieser Filtrierprozess wird im Abschnitt 9.3.1 im Detail aufgezeigt.

9.3.1 Ergebnis-Analyse

Zur Bestimmung der Expositions-Wahrscheinlichkeit im, in Abschnitt 7.2.1 als lichtrelevant eingestuften Szenario „Fahrzeug fährt bei *Dunkelheit* mit *hoher Geschwindigkeit* auf einer leeren (d.h. *niedrige Verkehrsdichte*) *außerörtlichen* Straße“ gilt es, die das Szenario maßgeblich bestimmenden Situations- und Fahrzeugzustandsmerkmale zu identifizieren. Im Falle dieses Beispiel-Szenarios werden folgende Merkmale und Merkmalsausprägungen als wesentlich eingestuft:

- Merkmale der Fahrsituation:
  - Helligkeit → dunkel
  - Ort → außerorts
  - Verkehrsdichte → niedrige Verkehrsdichte
- Merkmal des Fahrzeugzustands:
  - Fahrzeuggeschwindigkeit → fährt mit hoher Geschwindigkeit

Die weiteren das Gesamtmodell aufspannenden Merkmale *bauliche Trennung* und *Sichtbedingungen* mit ihren unterschiedlichen Merkmalsausprägungen spielen bezüglich des ganz speziellen Beispielszenarios eine eher untergeordnete Rolle und werden daher im Folgenden nicht differenziert betrachtet.
Im Hinblick auf die Ergebnis-Analyse bedeutet dies, dass die Eintrittswahrscheinlichkeiten des beschriebenen Szenarios *mit und ohne bauliche Trennung* bei *guten und*

schlechten Sichtbedingungen aufsummiert werden, um die Szenarien-Eintrittswahrscheinlichkeit, und damit die Expositionswahrscheinlichkeit im besagten einhüllenden Szenario zu bestimmen.
Durch Simulation und Analyse des in Anhang B zu Teilen abgebildeten Gesamtmodells lassen sich folgende Eintrittswahrscheinlichkeiten der Teilszenarien ableiten:

- **Sz154**[1] **(Fzg. 26)**: Fahrzeug fährt schnell, dunkel, gute Sicht, außerorts, bauliche Trennung, Verkehrsdichte niedrig (s. Abbildung 9.6 und Anhang B) $\rightarrow$ $P_{Sz154} = 0,012$
- **Sz166 (Fzg. 28)**: Fahrzeug fährt schnell, dunkel, gute Sicht, außerorts, keine bauliche Trennung, Verkehrsdichte niedrig $\rightarrow$ $P_{Sz166} = 0,014$
- **Sz178 (Fzg. 30)**: Fahrzeug fährt schnell, dunkel, schlechte Sicht, außerorts, bauliche Trennung, Verkehrsdichte niedrig $\rightarrow$ $P_{Sz178} = 0,002$
- **Sz190 (Fzg. 32)**: Fahrzeug fährt schnell, dunkel, schlechte Sicht, außerorts, keine bauliche Trennung, Verkehrsdichte niedrig $\rightarrow$ $P_{Sz190} = 0,004$

Die kumulierte Gesamtwahrscheinlichkeit des als kritisch angenommenen Szenarios , diese entspricht der gesuchten Expositionswahrscheinlichkeit, ergibt sich demzufolge zu:

$$\sum_{i=1}^{n} P_i = 0,032 = 3,2\% \tag{9.1}$$

Die mathematische Korrektheit des auf dem deterministischem Modell beruhenden Ergebnisses wird mittels des in Abbildung 9.7 dargestellten Ereignisbaumes (ETA) nachgewiesen. Auf die Überprüfung im Sinne einer Methoden-Validation wird in Abschnitt 9.3.2 eingegangen.

Mit Hilfe der Verhältnis-Gleichung 9.2 aus Tabelle 8.4 lässt sich der berechneten Expositionswahrscheinlichkeit nach ISO 26262 die Kategorie E3 zuweisen.

$$1\% \leq P \leq 10\% \rightarrow E3 \tag{9.2}$$

[1]Hinweis: Obwohl das das Gesamtmodell nur zwischen 128 verschiedenen Szenarien unterscheidet, werden im Folgenden Szenarien mit IDs>128 verwendet. Dies ist darauf zurückzuführen, dass das Modell stetig weiterentwickelt wurde (z.B. Streichung/Ergänzung von Szenarien) während die IDs einmal zu Beginn der Modellentwicklung vergeben wurden.

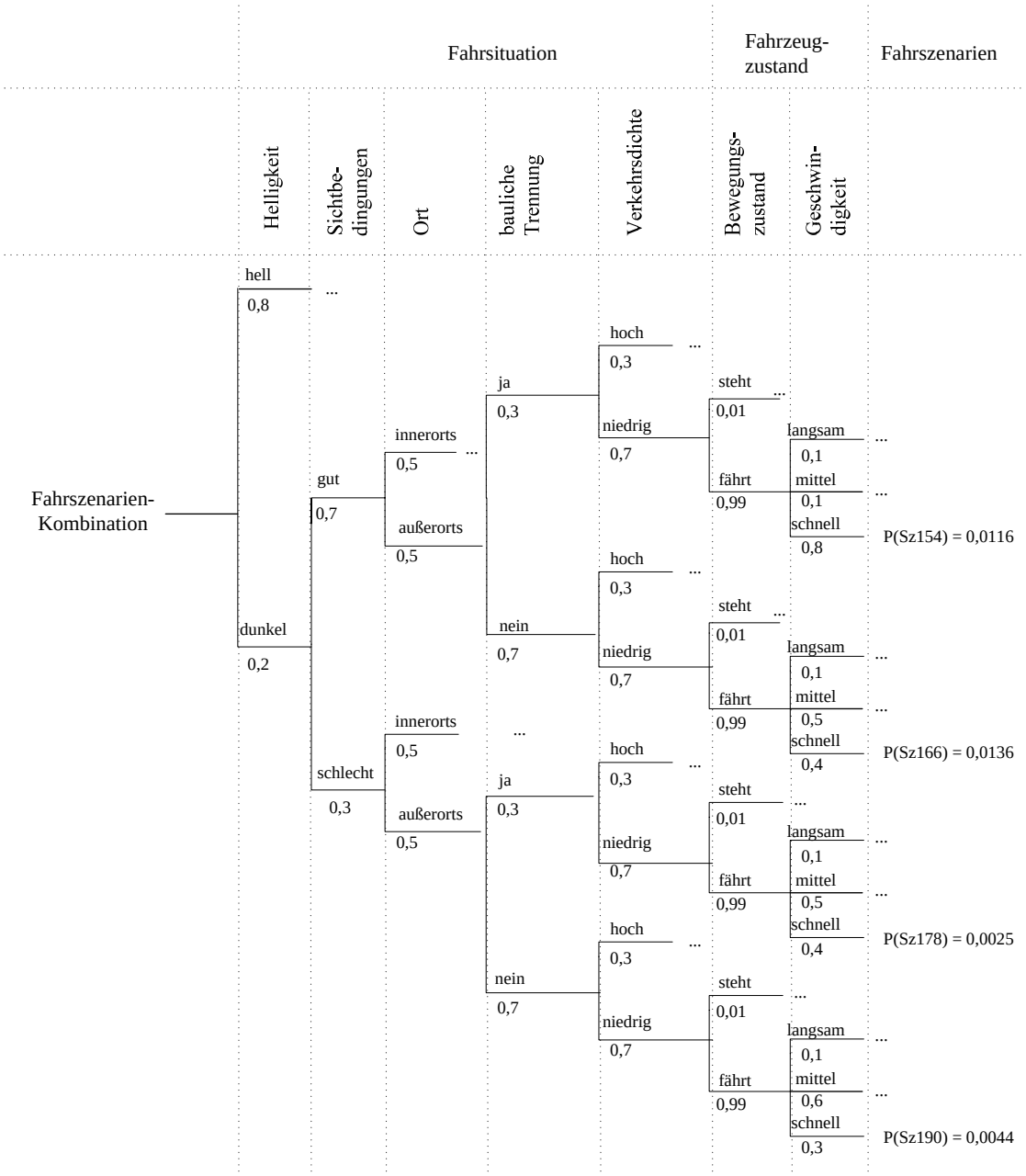


Abbildung 9.7: Validation der EmMORI-Methode - Ereignisbaumanalyse

9.3.2 Ergebnis-Plausibilisierung

Zur Plausibilitätsprüfung der Methode können die vorliegenden Analyse-Ergebnisse gegen die Klassifizierung der Expositionsdauer für das betrachtete Szenario aus Abschnitt 7.2.1 geprüft werden.

Auf diese Weise kann die Plausibilität der Methode, sowohl für das dargestellte Beispielszenario ($E_{Szenario-Schaetzung} = E_{Szenario-EmMORI}$), als auch für eine Vielzahl

weiterer stichprobenartig ausgewählter Szenarien aufgezeigt werden.
Hierbei wird in diesem Zusammenhang gezielt nur von einer Plausibilisierung und nicht von einer Validation im engeren mathematischen Sinne gesprochen, da es letztendlich streng genommen nicht möglich ist, objektive(re) Simulationsergebnisse gegen subjektive, also von der Emotionalität des Schätzenden abhängige, (Experten-) Schätzungen zu prüfen.
Da die Parameter C und S vor dem Hintergrund der in Abschnitt 8.1 diskutierten resultierenden Modellkomplexität weiterhin konventionell nach ISO 26262 bestimmt werden, ergibt sich für die Funktion „Abblendlicht“ im betrachteten Szenario „Fahrzeug fährt bei *Dunkelheit* mit *hoher Geschwindigkeit* auf einer leeren (d.h. *niedrige Verkehrsdichte*) *außerörtlichen* Straße“ analog zu der im ISO 26262 vorgeschlagenen Vorgehensweise, ein ASIL B (vgl. Abschnitt 7.2.1).
Bis hier hin wird davon ausgegangen, dass sich die zeitliche Veränderung realer Situationen durch deterministische Zeitbewertungen modellieren lässt. Um die sich in der Realität keineswegs immer deterministisch verändernden Umgebungseinflüsse realitätsnäher abzubilden, werden die in den merkmalsausprägenden Transitionen hinterlegten Raten aus Anhang C von nun an einer Exponentialverteilung folgend parametriert (s. hierzu auch Abschnitt 8.6).
Durch stochastische Simulation und Analyse des auf diese Weise parametrierten Petrinetz-Modells ergeben sich die zur weiteren Betrachtung aufzusummierenden Szenarien-Wahrscheinlichkeiten wie folgt:

- **Sz154 (Fzg. 26)**: Fahrzeug fährt schnell, dunkel, gute Sicht, außerorts, bauliche Trennung, Verkehrsdichte niedrig $\rightarrow P_{Sz154} = 0,0022$
- **Sz166 (Fzg. 28)**: Fahrzeug fährt schnell, dunkel, gute Sicht, außerorts, keine bauliche Trennung, Verkehrsdichte niedrig $\rightarrow P_{Sz166} = 0,0024$
- **Sz178 (Fzg. 30)**: Fahrzeug fährt schnell, dunkel, schlechte Sicht, außerorts, bauliche Trennung, Verkehrsdichte niedrig $\rightarrow P_{Sz178} = 0,0005$
- **Sz190 (Fzg. 32)**: Fahrzeug fährt schnell, dunkel, schlechte Sicht, außerorts, keine bauliche Trennung, Verkehrsdichte niedrig $\rightarrow P_{Sz190} = 0,0008$

Die kumulierte Gesamtwahrscheinlichkeit ergibt sich demzufolge zu:

$$\sum_{i=1}^{n} P_i = 0,006 = 0,6\% \tag{9.3}$$

Mit Hilfe der in ISO 26262 gegebenen Verhältnisgleichung (s. Gleichung 9.2) kann die berechnete Gesamtwahrscheinlichkeit der Kategorie E2 zugewiesen werden. Diese konservative Einordnung in die Klasse E2 erfolgt hierbei aufgrund der unzureichenden Spezifikation der Kategorie E1 (vgl. Tabelle 8.4). Diesbezüglich wird im Rahmen der Arbeit festgelegt, dass erst eine Wahrscheinlichkeit $P << 1\%$ eine Einordnung in die Klasse E1 rechtfertigt.
Basierend auf diesem Analyse-Ergebnis kann der Funktion „Abblendlicht“ für das betrachtete Szenario bei gleichbleibenden Parametern C und S eine Sicherheitsklasse von ASIL A zugewiesen werden.
Die vorliegenden Analyse-Ergebnisse der deterministisch parametrierten Modelle zeigen, dass die in Abschnitt 1.3 motivierte modellbasierte Schätz-Unterstützung erfolgreich zur objektiveren Abschätzung des Parameters E angewendet werden kann. Des Weiteren wird der die Expositionswahrscheinlichkeit reduzierende Effekt (vgl. Tabelle 9.1) des Übergangs zu realitätsnäheren stochastisch verteilten Raten (z.B. Exponentialverteilung) und dessen Einfluss auf die ASIL-Klassifizierung deutlich.
Dieser Effekt kommt aber nur dann so signifikant zum Tragen, wenn die ein Szenario

Tabelle 9.1: Analyseergebnisse im direkten Vergleich

	deterministisches Verhalten	**exponentielles Verhalten**
P_{Sz154}	0,012	0,0022
P_{Sz166}	0,014	0,0024
P_{Sz178}	0,002	0,0005
P_{Sz190}	0,004	0,0008
$\sum_{i=1}^{n} P_{Sz}$	0,032	0,006
E	3	2
ASIL (S3, C2, E...)	B	A

bestimmenden Merkmale tatsächlich durch exponentiell verteilte Merkmalsausprägungen, diese Annahme wurde für das Anwendungsbeispiel getroffen, abgebildet werden können.
Folgen die ein kritisches Szenario ausmachenden Merkmale in der Realität einer anderen stochastischen (z.B. Normal-, Weibull- oder Gamma-Verteilung) oder de-

terministischen Verteilung, so können diese den jeweiligen Merkmalen zugewiesen werden, und ein sehr genaues Abbild des sich in Realität ereignenden Szenarios, und der Expositionswahrscheinlichkeit im Szenario modelliert werden. In Abhängigkeit vom jeweiligen subjektiven *Referenzschätzer* und der erreichten Modellgenauigkeit kann es daher sowohl dazu kommen, dass die Analyse zu einer höheren, als auch zu einer niedrigeren, aber in jedem Falle einer objektiveren, als der geschätzten Expositionswahrscheinlichkeit kommt.

9.4 Diskussion der Ergebnisse

In diesem Kapitel wird die Anwendung der EmMORI-Methode an einem praxisnahen Beispiel aufgezeigt und plausibilisiert.
Hierbei wird zunächst ein deterministisches Verhalten der die Fahrszenarien bestimmenden Merkmale angenommen, um die mathematische Korrektheit des Modells mittels eines Ereignisbaums überprüfen zu können.
Auf Basis der Modellanalyse kann der Funktion „Abblendlicht“ im betrachteten Szenario ein ASIL B zugewiesen werden. Diese ASIL-Einstufung stimmt mit der in Abschnitt 7.2.1 auf herkömmliche Weise nach ISO 26262 bestimmten überein.
Um das reale Verhalten der sich selten rein deterministisch verändernden szenarienbestimmenden Konstituenten realitätsnäher abzubilden, wird den in den Transitionen hinterlegten Raten exponentielles Verhalten zugewiesen und ein erneute Monte-Carlo-Simulation durchgeführt. Basierend auf den Analyseergebnissen kann der Funktion bei gleichbleibenden Randbedingungen ein ASIL A zugeordnet, und eine normkonforme, da den Anforderungen der ISO 26262 entsprechende, auf objektiven Daten abgestütze ASIL-Reduktion, erreicht werden.
Aus dieser ASIL-Einstufung resultieren niedrigere Anforderungen an den Entwicklungsprozess (z.B. geringere Testabdeckung etc.) der Funktion und/oder die Systemarchitektur (z.B. einkanalige statt zweikanalige Auslegung etc.) des die Funktion realisierenden Systems. Hierdurch kann eine erhebliche Einsparung von Entwicklungskosten erreicht werden.
Nachvollziehbarerweise wird die Anwendung der EmMORI-Methode nicht zwangsweise immer zu einer ASIL-Reduktion führen. Die Objektivierung des Faktors E kann in Abhängkeit von den gewählten, in den merkmalsunterscheidenden Transitionen implementierten Verteilungen der Raten, ebenso zu konservativeren Ergeb-

nissen führen, als es die subjektive (Experten-)Schätzung getan hat. Dies kann eine Einstufung in eine höhere Sicherheitsklasse zur Folge haben, und damit höhere Anforderungen an den Entwicklungsprozess und die Systemarchitektur nach sich ziehen. Hieraus resultieren verständlicherweise von Entscheidungsträgern eher ungern gesehene steigende Entwicklungskosten.
Da die Einstufung in eine höhere Sicherheitsklasse jedoch letztendlich dafür sorgt, dass vom entwickelten System keine inakzeptablen Risiken ausgehen und das identifizierte Risikopotential auf der Analyse eines strukturierten Modellbildungs-Prozesses beruht, kann die EmMORI-Methode helfen, die steigenden Entwicklungskosten zu begründen.
Zudem dürfen die höheren Entwicklungkosten nicht isoliert betrachtet werden. Sie müssen vielmehr im Verhältnis zu möglichen, aus einer Fehlfunktion des entwickelten Systems resultierenden, Regressanforderungen oder aus Rückrufen entstehenden Kosten betrachtet werden.

Kapitel 10

Zusammenfassung, Diskussion und Ausblick

10.1 Ergebnisse und Diskussion

Der in ISO 26262 vorgeschlagene Ansatz zur Bewertung des von E/E/PE-Fahrzeugsystemen ausgehenden Risikos, und damit zur ASIL-Einstufung, basiert auf subjektiven Expertenschätzungen, die häufig sehr konservative Ergebnisse liefern und damit unnötig hohe Anforderungen an die Entwicklung und die Architektur der die Funktion realisierenden Systeme stellen.
Das Ziel der Objektivierung der vorgeschlagenenen Methode zur ASIL-Bestimmung erfordert einen methodischen Ansatz, der es ermöglicht, die den ASIL bestimmenden Parameter (S, E, und C) ganzheitlich und so realitätsnah wie möglich in ihrem Kontext abbilden zu können.
Basierend auf dieser Meta-Anforderung („realitätsnahe Abbildung“) werden Teilanforderungen (z.B. Darstellung von parallelen und/oder sequentiellen Prozessen) identifiziert, welche an die EmMORI-Technik gestellt werden und neben anderen Anforderungen (z.B. Übersichtlichkeit etc.) in einen paarweisen Vergleich zur Technik-Auswahl einfließen. Auf Basis des durchgeführten anforderungsgetriebenen paarweisen Vergleiches wird die Petrinetz-Analyse als die den Anforderungen in höchstem Maße gerecht werdende Technik identifziert.
Zur realtitätsnahen Modellierung der den ASIL beeinflussenden Faktoren bedarf es allerdings nicht nur eines umfangreichen Verständnisses der in ISO 26262 vorgeschlagenen Methodik, sondern zusätzlicher terminologischer Kenntnisse über den

inhaltlichen Umfang, welcher sich hinter den potenziell modellgestützt objektivierbaren Parametern verbirgt, und deren Einordnung in den Kontext der funktionalen Sicherheit.
Das entwickelte, auf dem Beschreibungsmittel *Petrinetz* basierende, generische Modellkonzept mit den beliebig erweiterbaren bzw. anpassbaren Modell-Modulen zur Abbildung von Fahrsituationen bzw. Umgebungs-Situationen, Fahrzeugzuständen und Fahrszenarien konnte erfolgreich zur Objektivierung der Bestimmung des ASIL für die praxisnahe Beispielfunktion *Abblendlicht* angewendet werden.
Die in diesem Falle wissenschaftlich fundiert erbrachte ASIL-Reduktion führt zu deutlich geringeren, von der ISO 26262 an die Funktionsentwicklung gestellten Anforderungen, wodurch erhebliche Einsparpotenziale hinsichtlich der Entwicklungskosten erreicht werden können.
Die vorgestellte Methode wird nachvollziehbarerweise nicht immer zu einer ASIL-Reduktion, sondern kann in Abhängigkeit von den zuvor durchgeführten subjektiven Expertenschätzungen auch zu einer ASIL-Erhöhung führen. Da die Einstufung in eine höhere Sicherheitsklasse jedoch dafür sorgt, dass vom entwickelten System keine inakzeptablen Risiken ausgehen und das identifizierte Risikopotential auf der Analyse eines strukturierten Modellbildungs-Prozesses beruht, kann die EmMORI-Methode helfen steigende Entwicklungskosten gegenüber Entscheidungsträgern zu begründen. Zudem dürfen die höheren Entwicklungskosten nicht isoliert betrachtet werden. Sie müssen vielmehr ins Verhältnis zu möglichen, aus einer Fehlfunktion des entwickelten Systems resultierenden, Regressanforderungen oder aus Rückrufen entstehenden Kosten gesetzt werden.

10.2 Ausblick

Da sich diese Arbeit aus Gründen der Vielfalt und der Komplexität, der die Parameter *Schadensausmaß (S)* und *Kontrollierbarkeit (C)* charakterisierenden Faktoren, auf die Objektivierung der *Expositions-Wahrscheinlichkeit (E)* beschränkt, sind weiterführende Arbeiten insbesondere hinsichtlich der Objektivierung der Schätzungen der Parameter S und C denkbar. In beiden Fällen scheinen interdisziplinäre Ansätze zielführend.
So gilt es im Zuge der Objektivierung des Faktors C insbesondere die ingenieursmäßige Sicht mit physiologischen und psychologischen Aspekten zu verknüpfen, um

auch die Mensch-Maschine-Interaktion geeignet abbilden und bewerten zu können. Hinsichtlich einer angestreben Objektivierung des Faktors S ist eine tiefergehende Untersuchung der zu entwickelnden Funktionen mit dem Hintergrundwissen der Unfallforschung unabdingbar.
Der Einsatz der EmMORI-Methode ist im Rahmen dieser Arbeit zwar auf die Objektivierung der ASIL-Bestimmung beschränkt. Aufgrund der generischen Struktur der Modell-Module ist eine Überführung des Ansatzes in andere Branchen – die Einflüsse subjektiver Schätzungen sind schließlich keinesfalls automobilspezifisch – ohne großen Aufwand möglich.
Ein weiteres wichtiges Forschungs- und Entwicklungsfeld stellt die Implementierung einer methodenspezifischen, aber nicht branchenspezifischen Toolunterstützung dar. Die Hauptanforderung ist dabei, dass auch ein Anwender ohne allzu große Petrinetz-Expertise befähigt wird, Fahrsituationen und Fahrzeugzustände zu modellieren und zu Fahrszenarien zu verknüpfen. Dies beispielsweise, indem der Anwender basierend auf einem generischen Merkmalskatalog eine strukturierte Liste von funktionsrelevanten Merkmalsausprägungen von Umgebungsmerkmalen und Fahrzeugzuständen erstellt und diese automatisch in simulations- und analysefähige Modelle überführt werden, welche dann nur noch geeignet parametriert werden.

Anhang A

Paarweiser Vergleich der Techniken

Tabelle A.1: Paarweiser Vergleich – Standardisierung/Normkonformität

Standardisierung/ Normkonformität	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	1	1	1	1	1	6	18	0,86	1
FMEA	1	X	1	1	1	1	1	6	18	0,86	1
ETA	1	1	X	1	1	1	1	6	18	0,86	1
FTA(RBD)	1	1	1	X	1	1	1	6	18	0,86	1
Markov-Modell	1	1	1	1	X	1	1	6	18	0,86	1
Petrinetz	1	1	1	1	1	X	1	6	18	0,86	1
Entscheidungstabelle	1	1	1	1	1	1	X	6	18	0,86	1

Tabelle A.2: Paarweiser Vergleich – Aktualisierbarkeit/Anpassungsfähigkeit

Aktualsierbarkeit/ Anpassungsfähigkeit	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	2	2	2	2	2	1	11	23	0,82	7
FMEA	0	X	1	1	1	1	1	5	17	0,87	2
ETA	0	1	X	1	1	1	1	5	17	0,87	2
FTA(RBD)	0	1	1	X	1	1	1	5	17	0,87	2
Markov-Modell	0	1	1	1	X	1	1	5	17	0,87	2
Petrinetz	0	1	1	1	1	X	0	4	16	0,87	1
Entscheidungstabelle	1	1	1	1	1	2	X	7	19	0,85	6

Tabelle A.3: Paarweiser Vergleich – Simulation und Analyse

Simulation und Analyse	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	2	2	2	2	1	10	22	0,83	6
FMEA	1	X	2	2	2	2	1	10	22	0,83	6
ETA	0	0	X	1	2	2	0	5	17	0,87	3
FTA(RBD)	0	0	1	X	2	2	0	5	17	0,87	3
Markov-Modell	0	0	0	0	X	2	1	3	15	0,88	2
Petrinetz	0	0	0	0	0	X	1	1	13	0,90	1
Entscheidungstabelle	1	1	2	2	1	1	X	8	20	0,84	5

Tabelle A.4: Paarweiser Vergleich – Formalisierungsgrad

Formalisierungs-grad	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	2	2	2	2	2	11	23	0,82	6
FMEA	1	X	2	2	2	2	2	11	23	0,82	6
ETA	0	0	X	1	1	1	1	4	16	0,87	1
FTA(RBD)	0	0	1	X	1	1	1	4	16	0,87	1
Markov-Modell	0	0	1	1	X	1	1	4	16	0,87	1
Petrinetz	0	0	1	1	1	X	1	4	13	0,87	1
Entscheidungstabelle	0	0	1	1	1	1	X	4	16	0,87	1

Tabelle A.5: Paarweiser Vergleich – Toolunterstützung

Tool-unterstützung	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	2	2	2	2	2	2	12	24	0,81	7
FMEA	0	X	1	1	1	1	1	5	17	0,87	1
ETA	0	1	X	1	1	1	1	5	17	0,87	1
FTA(RBD)	0	1	1	X	1	1	1	5	17	0,87	1
Markov-Modell	0	1	1	1	X	1	1	5	17	0,87	1
Petrinetz	0	1	1	1	1	X	1	5	17	0,87	1
Entscheidungstabelle	0	1	1	1	1	1	X	5	17	0,87	1

Tabelle A.6: Paarweiser Vergleich – Nebenläufigkeit

Nebenläufigkeit	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	1	1	1	2	1	7	19	0,85	5
FMEA	1	X	1	1	1	2	1	7	19	0,85	5
ETA	1	1	X	1	1	2	0	6	18	0,86	2
FTA(RBD)	1	1	1	X	1	2	0	6	18	0,86	2
Markov-Modell	1	1	1	1	X	2	0	6	18	0,86	2
Petrinetz	0	0	0	0	0	X	0	0	12	0,90	1
Entscheidungstabelle	1	1	2	2	2	2	X	10	22	0,83	7

Tabelle A.7: Paarweiser Vergleich – Sequentialität

Sequentialität	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	2	2	2	2	1	10	22	0,83	5
FMEA	1	X	2	2	2	2	1	10	22	0,83	5
ETA	0	0	X	0	0	1	0	1	13	0,90	1
FTA(RBD)	0	0	2	X	1	2	0	5	17	0,87	3
Markov-Modell	0	0	2	1	X	2	0	5	17	0,87	3
Petrinetz	0	0	1	0	0	X	0	1	13	0,90	1
Entscheidungstabelle	1	1	2	2	2	2	X	10	22	0,83	5

Tabelle A.8: Paarweiser Vergleich – Kausalität

Kausalität	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	2	2	2	1	2	2	11	23	0,82	7
FMEA	0	X	1	1	1	1	1	5	17	0,87	4
ETA	0	1	X	1	1	1	0	4	16	0,87	3
FTA(RBD)	0	1	1	X	0	1	0	3	15	0,88	1
Markov-Modell	1	1	1	2	X	2	0	7	19	0,85	5
Petrinetz	0	1	1	1	0	X	0	3	15	0,88	1
Entscheidungstabelle	0	1	2	2	2	2	X	9	21	0,83	6

Tabelle A.9: Paarweiser Vergleich – Übersichtlichkeit

Übersichtlichkeit	HAZOP	FMEA	ETA	FTA(RBD)	Markov-Modell	Petrinetz	Entscheidungstabelle	Zeilensumme	normierte Zeilensumme (+12)	relative Bedeutung	Rang
HAZOP	X	1	2	2	1	1	2	9	21	0,83	6
FMEA	1	X	2	2	1	1	1	8	20	0,84	5
ETA	0	0	X	1	0	0	0	1	13	0,90	1
FTA(RBD)	0	0	1	X	0	0	0	1	13	0,90	1
Markov-Modell	1	1	2	2	X	2	1	9	21	0,83	6
Petrinetz	1	1	2	2	0	X	1	7	19	0,85	3
Entscheidungstabelle	0	1	2	2	1	1	X	7	19	0,85	3

Anhang B

Anwendungsbeispiel im Modell

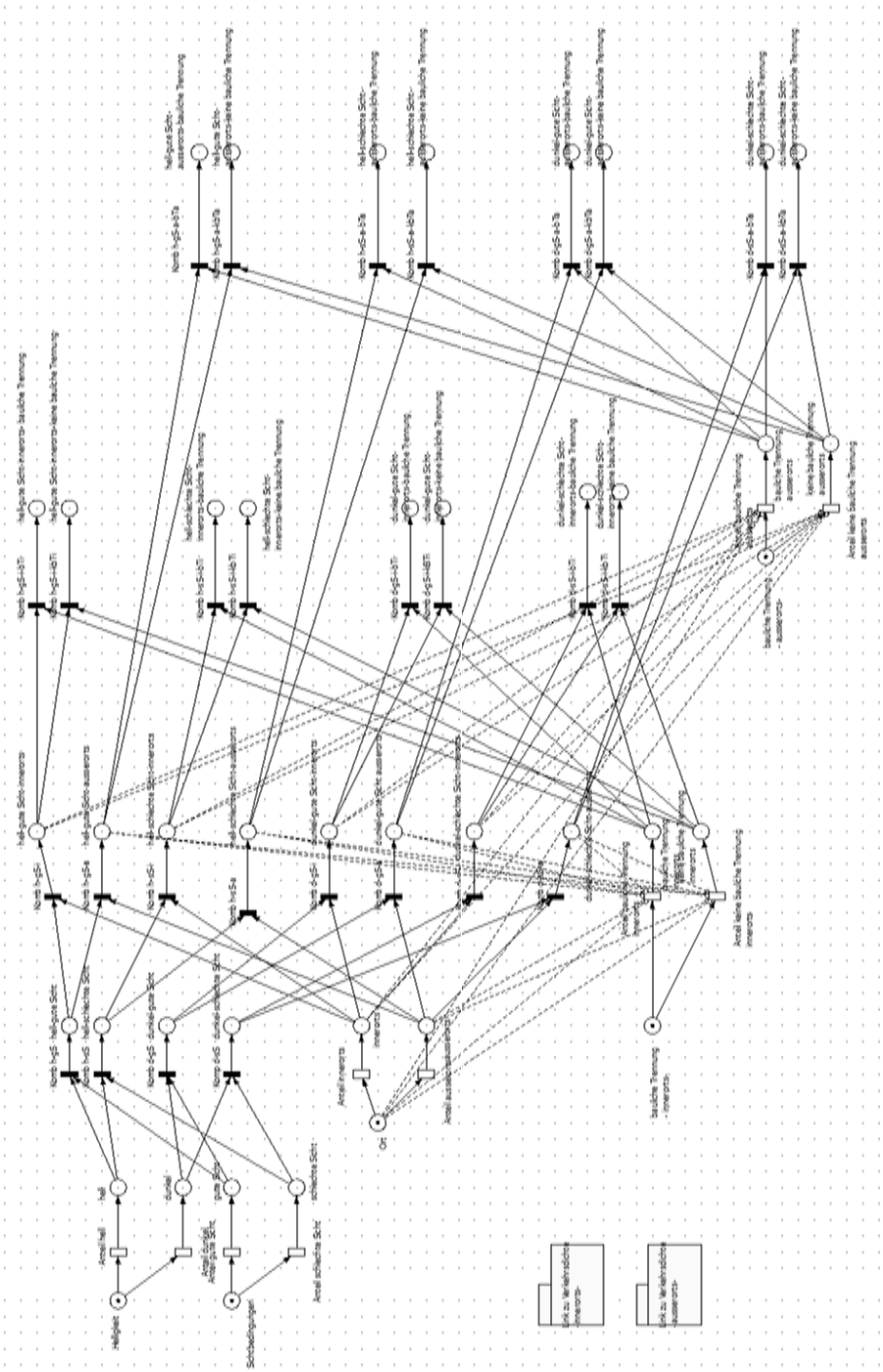


Abbildung B.1: Anwendungsbeispiel-Environment

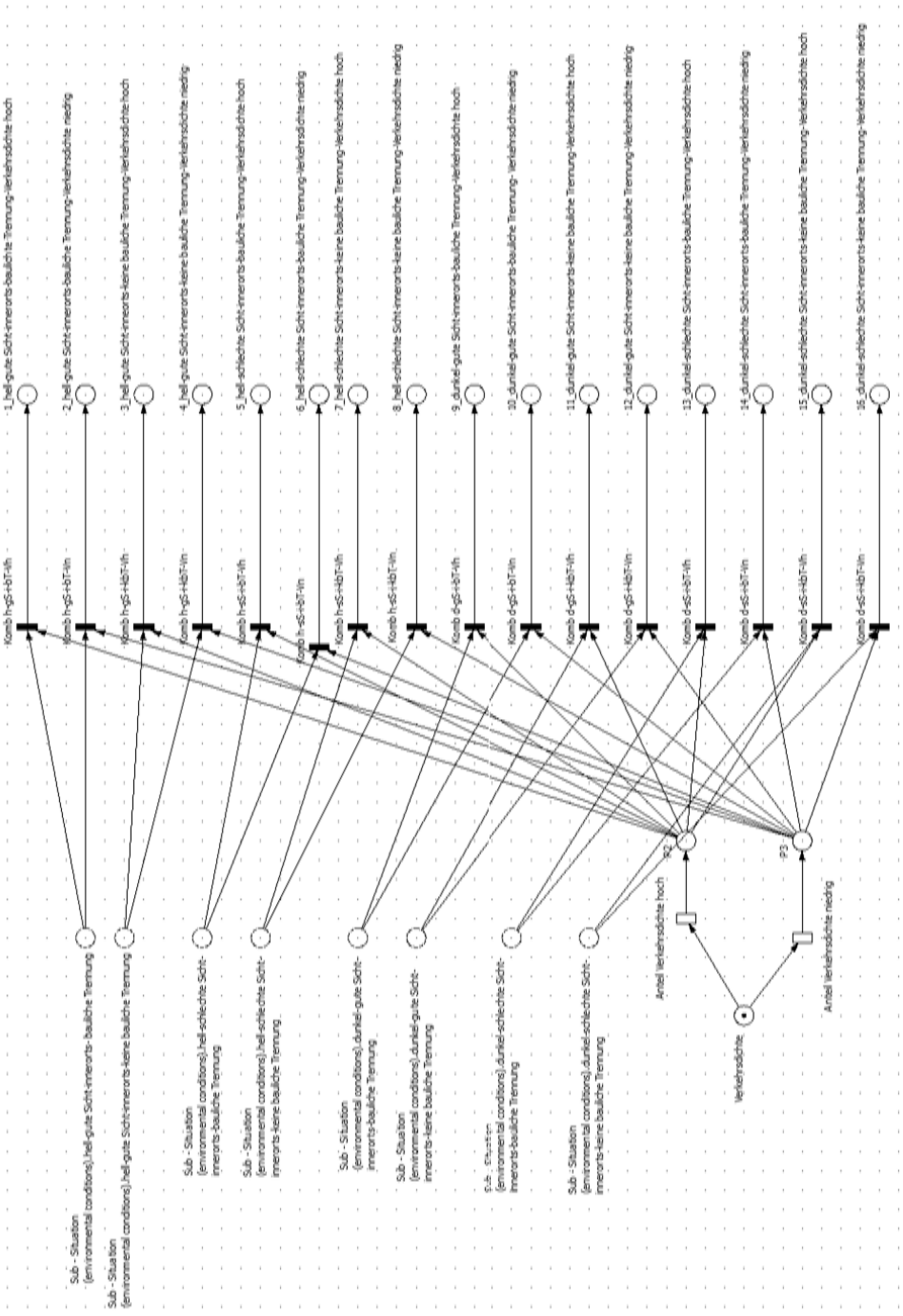


Abbildung B.2: Situationsgenerierung innerorts

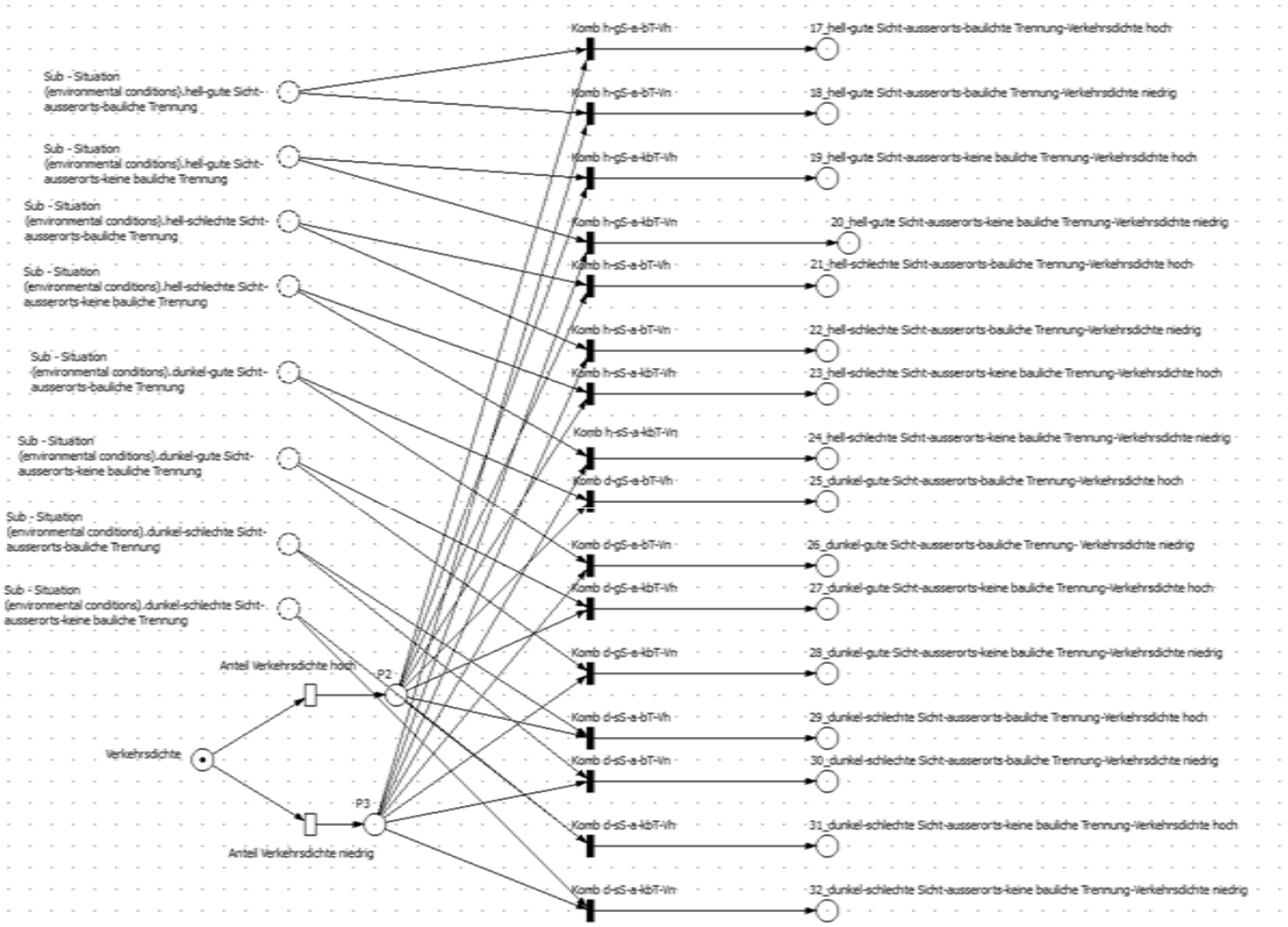


Abbildung B.3: Situationsgenerierung ausserorts

Anhang C

Modellparameter im Überblick

(Sub-)Netz	Merkmal	Parameter	Wert	Quelle/Anmerkungen
environmental conditions	Helligkeit	Anteil hell	0,8	…, obwohl der Anteil der Nachtfahrten lediglich 20 Prozent der Gesamtfahrleistung beträgt [http://www.bast.de/nn_40694/DE/Publikationen/Infos/2009-2008/03-2008.html]
		Anteil dunkel	0,2	
	Sichtbedingungen	Anteil gute Sicht	0,7 (0,94)	Die Zahl der Nebeltage hingegen blieb mit jährlich im Schnitt 23 Tagen unverändert. Darauf hat der ACE Auto Club Europa nach Auswertung von Erhebungen des Statistischen Bundesamtes am Donnerstag in Stuttgart hingewiesen. [http://www.autonews-123.de/nebelunfalle-werden-weniger-%E2%80%93-zahl-der-nebeltage-bleibt-jedoch-gleich/] ACHTUNG: Statistik: nur Nebel als Sichtbehinderung eingestuft; im Modell schlechter eingestuft, da auch Regen etc. Sichtbehindern kann
		Anteil schlechte Sicht	0,3 (0,06)	
	Ort	Anteil innerorts	0,5	Bundesautobahnen 214,8 Bundesstraßen außerorts 108,6 alle Straßen 686 (in Mrd. Fzg.-Km) [http://www.bast.de/nn_42244/DE/Presse/Pressemitteilungen/Downloads/presse-15-04,templateId=raw,property=publicationFile.pdf/presse-15-04.pdf] ODER nach Straßenkilometer: http://www.statistik-hessen.de/themenauswahl/verkehr-umwelt/landesdaten/strassen/laenge-der-oeffentlichen-strassen/index.html
		Anteil ausserorts	0,5	
	bauliche Trennung - innerorts -	Anteil bauliche Trennung innerorts	0,1	Schätzung
		Anteil keine bauliche Trennung innerorts	0,9	Schätzung

Abbildung C.1: Modell-Parameter I

(Sub-)Netz	Merkmal		Parameter	Wert		Quelle/Anmerkungen
environmental conditions	bauliche Trennung - ausserorts -		Anteil bauliche Trennung ausserorts	0,3		Schätzung basierend auf: http://www.statistik-hessen.de/themenauswahl/verkehr-umwelt/landesdaten/strassen/laenge-der-oeffentlichen-strassen/index.html
			Anteil keine bauliche Trennung ausserorts	0,7		
Link zu Verkehrsdichte - innerorts -	Verkehrsdichte - innerorts -		Anteil Verkehrsdichte hoch (innerorts)	0,6		Schätzung
			Anteil Verkehrsdichte niedrig (innerorts)	0,4		Schätzung
Link zu Verkehrsdichte - ausserorts -	Verkehrsdichte - ausserorts -		Anteil Verkehrsdichte hoch (ausserorts)	0,3		Schätzung
			Anteil Verkehrsdichte niedrig (ausserorts)	0,7		Schätzung
Fahrzeugzustand 1: 1_hell-gute Sicht-innerorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 2: 2_hell-gute Sicht-innerorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,2	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 3: 3_hell-gute Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 4: 4_hell-gute Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Annahme: ob bauliche Trennung oder keine bauliche Trennung, hat auf das Fahrverhalten keinen Einfluss
		Anteil fahren	Anteil langsam	0,8	0,2	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,2	Schätzung

Abbildung C.2: Modell-Parameter II

(Sub-)Netz	Merkmal		Parameter	Wert		Quelle/Anmerkungen
Fahrzeugzustand 5: 5_hell-schlechte Sicht-innerorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,5	Schätzung
			Anteil mittel		0,4	Schätzung
			Anteil schnell		0,1	Schätzung
Fahrzeugzustand 6: 6_hell-schlechte Sicht-innerorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 7: 7_hell-schlechte Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,5	Schätzung
			Anteil mittel		0,4	Schätzung
			Anteil schnell		0,1	Schätzung
Fahrzeugzustand 8: 8_hell-schlechte Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 9: 9_dunkel-gute Sicht-innerorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Annahme: Dunkelheit beeinflusst das Fahrverhalten innerorts quasi nicht
		Anteil fahren	Anteil langsam	0,6	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 10: 10_dunkel-gute Sicht-innerorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,2	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 11: 11_dunkel-gute Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 12: 12_dunkel-gute Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,2	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 13: 13_dunkel-schlechte Sicht-innerorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,5	Schätzung
			Anteil mittel		0,4	Schätzung
			Anteil schnell		0,1	Schätzung

Abbildung C.3: Modell-Parameter III

(Sub-)Netz	Merkmal		Parameter	Wert		Quelle/Anmerkungen
Fahrzeugzustand 14: 14_dunkel-schlechte Sicht-innerorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 15: 15_dunkel-schlechte Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,4		Schätzung
		Anteil fahren	Anteil langsam	0,6	0,5	Schätzung
			Anteil mittel		0,4	Schätzung
			Anteil schnell		0,1	Schätzung
Fahrzeugzustand 16: 16_dunkel-schlechte Sicht-innerorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,2		Schätzung
		Anteil fahren	Anteil langsam	0,8	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 17: 17_hell-gute Sicht-ausserorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		mit: http://www.zahlenspiegel.net/59/24-tage-im-stau
		Anteil fahren	Anteil langsam	0,9	0,1	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,3	Schätzung
Fahrzeugzustand 18: 18_hell-gute Sicht-ausserorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,1	Schätzung
			Anteil schnell		0,8	Schätzung
Fahrzeugzustand 19: 19_hell-gute Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,1	Schätzung
			Anteil mittel		0,7	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 20: 20_hell-gute Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,4	Schätzung
Fahrzeugzustand 21: 21_hell-schlechte Sicht-ausserorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,3	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 2: 22_hell-schlechte Sicht-ausserorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,4	Schätzung
Fahrzeugzustand 23: 23_hell-schlechte Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,3	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,1	Schätzung

Abbildung C.4: Modell-Parameter IV

(Sub-)Netz	Merkmal		Parameter	Wert		Quelle/Anmerkungen
Fahrzeugzustand 24: 24_hell-schlechte Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,3	Schätzung
Fahrzeugzustand 25: 25_dunkel-gute Sicht-ausserorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,1	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,3	Schätzung
Fahrzeugzustand 26: 26_dunkel-gute Sicht-innerorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,1	Schätzung
			Anteil schnell		0,8	Schätzung
Fahrzeugzustand 27: 27_dunkel-gute Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,1	Schätzung
			Anteil mittel		0,7	Schätzung
			Anteil schnell		0,2	Schätzung
Fahrzeugzustand 28: 28_dunkel-gute Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,4	Schätzung
Fahrzeugzustand 29: 29_dunkel-schlechte Sicht-ausserorts-bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,3	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,1	Schätzung
Fahrzeugzustand 30: 30_dunkel-schlechte Sicht-ausserorts-bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,5	Schätzung
			Anteil schnell		0,4	Schätzung
Fahrzeugzustand 31: 31_dunkel-schlechte Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte hoch	Bewegungszustand	Anteil stehen		0,1		Schätzung
		Anteil fahren	Anteil langsam	0,9	0,3	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,1	Schätzung
Fahrzeugzustand 32: 32_dunkel-schlechte Sicht-ausserorts-keine bauliche Trennung-Verkehrsdichte niedrig	Bewegungszustand	Anteil stehen		0,01		Schätzung
		Anteil fahren	Anteil langsam	0,99	0,1	Schätzung
			Anteil mittel		0,6	Schätzung
			Anteil schnell		0,3	Schätzung

Abbildung C.5: Modell-Parameter V

Literaturverzeichnis

[AB09] Abendroth, Bettina ; Bruder, Ralph: Die Leistungsfähigkeit des Menschen für die Fahrzeugführung. In: *Handbuch Fahrerassistenzsysteme.* Vieweg+Teubner, 2009

[ABDM09] Ahlgrimm, Jörg ; Burg, Heinz ; Dettinger, Jürgen ; Moser, Andreas: Fußgängerunfälle. In: *Handbuch Verkehrsunfallrekonstruktion – Unfallaufnahme, Fahrdynamik, Simulation.* Vieweg+Teubner, 2009

[AG07] Asmussen, S. ; Glynn, P.: *Stochastic Simulation.* Springer, 2007

[Aut09] Autobild: *Führerscheinkosten in Europa – Billig-Lappen in Bulgarien.* http://www.autobild.de/artikel/fuehrerscheinkosten-in-europa_996769.html, 2009. Letzter Aufruf: 08/2010

[Bae08] Baer, Rudolf: *Vom richtigen Umgang mit Risiken* http://www.bsg.ch/fileadmin/downloads/Vom_richtigen_Umgang_mit_Risiken.pdf. – Letzter Aufruf: 03/2010

[Bas96] Basler, Ernst : *Bewertungsverfahren für Sicherheitsfragen im Eisenbahnbetrieb.* Bundesministerium für Verkehr, Bonn, 1996

[Bast99] *Merkblatt für die Ausstattung von Verkehrsrechnerzentralen und Unterzentralen.* Bundesanstalt für Straßenwesen (Bast), 1999

[Bau03] Baumann, Frank Wolfgang: *Untersuchungen zur dynamischen Rollstabilität von Personenkraftwagen*, TU Darmstadt, Diss., 2003

[Bau96] Baumgarten, Bernd: *Petri-Netze – Grundlagen und Anwendungen.* Spektrum Akademischer Verlag, 1996

[Bep08] Bepperling, Sonja-Lara: *Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik*, TU Braunschweig, Diss., 2008

[BHKP09] Bergholz, Janine ; Henze, Roman ; Kücükay, F. ; Pawellek, T.: Was kann der Fahrer leisten? In: *AAET 2009 - Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel*, Gesamtzentrum für Verkehr e.V., 2009, S. 368–389

[Beu07] Beucher, Ottmar: *Wahrscheinlichkeitsrechnung und Statistik mit MATLAB*. Springer, 2007

[BJ04] Beine, M. ; Jungmann, M.: Einsatz von automatischer Code-Generierung für die Entwicklung von sicherheitkritischer Software. In: *Embedded World* 2004

[BL04] Bertsche, Bernd ; Lechner, Gisbert: *Zuverlässigkeit im Fahrzeug- und Maschinenbau: Ermittlung von Bauteil- und System-Zuverlässigkeiten*. Springer-Verlag Berlin Heidelberg New York, 3., überarbeitete und erweiterte Auflage, 2004

[BM09] Berg, Heinz ; Moser, Andreas: Systematik der Fahrzeugtechnik. In: *Handbuch Verkehrsunfallrekonstruktion – Unfallaufnahme, Fahrdynamik, Simulation*. Vieweg+Teubner, 2009

[BS02] Bikker, Gert; Schroeder, Martin: *Methodische Anforderungsanalyse und automatisierter Entwurf sicherheitsrelevanter Eisenbahnleitsysteme mit kooperierenden Werkzeugen*, TU Braunschweig, Diss., 2002

[Bir07] Birolini, Alessandro: *Reliability Engineering – Theory and Practice*. Springer Verlag, 2007

[BFGP03] Bobbio, Andrea ; Franceschinis, Giuliana ; Gaeta, Rossano ; Protinale, Luigi: Parametric Fault Tree for the Dependability Analysis of Redundant Systems and Its High-Level Petri Net Semantics. In: *IEEE Transactions on Software Engineering* 29 (2003), Nr. 3

[Bod06] Bodendorf, Freimut: *Daten- und Wissensmanagement*. Springer, 2006

[Bör06] BÖRCSÖK, Josef: *Funktionale Sicherheit – Grundzüge sicherheitstechnischer Systeme*. Hüthig, 2006

[Bra04] BRABAND, Jens: Risikoakzeptanzkriterien und -bewertungsmethoden. In: *Signal + Draht* 96 (2004), S. 6–9

[Bra05] BRABAND, Jens: Ein semi-quantitativer Ansatz zur Risikoanalyse in der Eisenbahnautomatisierung. In: *Signal + Draht* 10 (2005)

[Bra06] BRABAND, Jens: *Risikoanalysen in der Eisenbahn-Automatisierung*. Tetzlaff-Hestra GmbH+Co, KG., 2006

[BC09] BUCHHOLZ, Peter ; CLAUSEN, Uwe: *Große Netze der Logistik*. Springer, 2009

[Bud06] BUDIN, Gerhard: Kommunikation in Netzwerken – Terminologiemanagement. In: *Semantic Web – Wege zur vernetzten Wissensgesellschaft*. Springer, 2006

[BGK+09] BURG, Heinz ; GEIGL, Bertram C. ; KRAMER, Florian ; MOSER, Andreas ; STEFFAN, Hermann: Biomechanik. In: *Handbuch Verkehrsunfallrekonstruktion – Unfallaufnahme, Fahrdynamik, Simulation*. Vieweg+Teubner, 2009

[Cho99] CHOUIKHA, M.: *Entwurf diskret-kontinuierlicher Steuerungssysteme - Modellbildung, Analyse und Synthese mit hybriden Petrinetzen*, TU Braunschweig, Diss., 1999

[CJS98] CHOUIKHA, M. ; JANHSEN, A. ; SCHNIEDER, E.: Klassifikation und Bewertung von Beschreibungsmitteln für die Automatisierungstechnik. In: *at - Automatisierungstechnik* 46 (1998), Nr. 12

[DES09] DESTATIS: *Polizeilich erfasste Unfälle – Unfälle und Verunglückte im Straßenverkehr*. http://www.destatis.de, 2009. – letzter Abruf: 03/2010

[DSS10] DETERING, Stefan ; SCHNIEDER, Lars ; SCHNIEDER, Eckehard: Two-Level Validation and Data Acquisition for Microscopic Traffic Simulation Models. In: *International Journal On Advances in Software* (2010).

[Dil00] Dill, Christoph: *Paarweiser Vergleich.* http://imihome.imi.uni-karlsruhe.de/npaarweiser_vergleich_b.html, 2000. – Letzter Aufruf: 03/2010

[DIN25419] DIN 25419: Ereignisablaufanalyse – Verfahren, graphische Symbole und Auswertung / DIN. 1985.

[DIN50129] DIN EN 50129: Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik / CENELEC. 2003.

[ISO9000] DIN EN ISO 9000: Qualitätsmanagementsysteme – Grundlagen und Begriffe / DIN. 2005.

[DIN FB 144] DIN FB 144: Sicherheit, Vorsorge und Meidung in der Technik / DIN. 2005.

[DIN60812] DIN EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen - Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) / DIN. 2006.

[DIN61165] DIN EN 61165: Anwendung des Markoff-Verfahrens / DIN. 2007.

[DIN61025] DIN EN 62502: Fehlzustandsbaumanalyse / DIN. 2007.

[DIN45020] DIN 45020: Normung und damit zusammenhängende Tätigkeiten / DIN. 2007.

[DIN62502] DIN IEC 62502: Verfahren zur Analyse der Zuverlässigkeit - Ereignisbaumanalyse / DIN. 2008.

[DIN60050] DIN 60050: Internationales Elektrotechnisches Wörterbuch / DIN. 2009.

[Dre09] Drewes, Jörn: *Verkehrssicherheit im systemischen Kontext*, TU Braunschweig, Diss., 2009

[DTGN84] Dugan, J. ; Trivedi, K. ; Geist, R. ; Nicola, V.: Extended stochastic petri nets: Applications and analysis. In: *Proceeding Performance'84*, 1984

[DVR06] *Fahrerassistenzsysteme als „beste Beifahrer“*. www.dvr.de, 2006. – letzter Abruf: 01/2008

[DVR07] *Im Blickpunkt – Elektronische Beifahrer auf Herz und Nieren getestet.* www.dvr.de, 2007. – letzter Abruf: 01/2008

[EWGN08] Ehmanns, D. ; Wallentowitz, H. ; Gelau, C. ; Nicklisch, F.: Zukünftige Entwicklungen von Fahrerassistenzsystemen und Methoden zu deren Bewertung. In: *Tagungsband zum 9. Aachener Kolloquium Fahrzeug- und Motorentechnik*, 2008

[ES99] Einer, Stefan ; Schnieder, Eckehard: Formale Techniken für die Eisenbahnsicherungstechnik - Anforderungskatalog. In: *Signal + Draht* 91 (1999), Nr. 10

[EN50129] EN 50129: Bahnanwendungen - Sicherheitsrelevante elektronische Systeme für die Signaltechnik / CEN. 1998.

[Eri05] Ericson, C.A.: *Hazard analysis techniques for system safety.* Wiley-Interscience, 2005

[Ern08] Ernst, H.: *Grundkurs Informatik. Grundlagen und Konzepte für die erfolgreiche IT-Praxis – Eine umfassende, praxisorientierte Einführung.* Vieweg-Teubner, 2008

[EU08] *Daytime Running Lights for all new vehicles from 2011 to increase road safety.* IP/08/1394, Brüssel 2008.

[Fay99] Fay, Alexander: *Wissensbasierte Entscheidungsunterstützung für die Disposition im Schienenverkehr – Eine Anwendung von Fuzzy-Petrinetzen*, TU Braunschweig, Diss., 1999

[Fro06] Frohnhoff, Stephan: Große Softwareprojekte – Aufwandsschätzung mit „Use Case Points“. In: *Informatik Spektrum* 31 (2006), S. 566– 575

[FZV06] Bundesministerium der Justiz: *Verordnung über die Zulassung von Fahrzeugen zum Straßenverkehr.* 2006

[Ger94] German, R.: *Analysis of Stochastic Petri Nets with Non-Exponentially Distributed Firing Times*, TU Berlin, Diss., 1994

[GG49] *Grundgesetz – Verfassung der Bundesrepublik Deutschland.* 1949

[Gei91] Geiger, H. ; Zeller, H.; Röthlisberger, G.: Starkniederschläge des schweizerischen Alpen- und Alpenrandgebietes. In: *Eidgenössische Forschungsanstalt für Wald, Schnee und Landschaft* (1991), Bd. 7

[GGS09] Gelau, Christhard ; Gasser, Tom M. ; Seeck, Andre: Fahrerassistenz und Verkehrssicherheit. In: *Handbuch Fahrerassistenzsysteme.* Vieweg+Teubner, 2009

[GV02] Girault, C.; Valk, R.: *Petri Nets for Systems Engineering.* Springer, 2002

[Glä07] Gläser, Stefan: *Logische Analyse offener Kommunikationsarchitekturen für Kraftfahrzeuge*, TU Braunschweig, Diss., 2007

[Go09] Gombert, B.: Entwicklung von mechatronischen Produkten, besonders im Hinblick auf die funktionale Sicherheit. In: *Automation Valley Nordbayern* 2009

[Haf05] Haffner, Andreas: *Ein Modell zur Bestimmung der monetären Einsparungspotenziale bei der Durchführung einer Fehlermöglichkeits- und Einflussanalyse (FMEA)*, Universität Stuttgart, Diss., 2005

[Hän08] Hänsel, Frank: *Zur Formalisierung technischer Normen*, TU Braunschweig, Diss., 2008

[Har08] Harbig, Nathalie: *Risiko-/Zuverlässigkeitsbasierte Untersuchung von Systemarchitekturen moderner Fahrerassistenzsysteme*, TU Braunschweig, Diplomarbeit, 2008

[Hau05] Haupt, Heiko: Mit voller Kraft in die Eisen. In: *Spiegel Online* (2005)

[HL98] Hurrelmann, Klaus ; Laaser, Ulrich: *Handbuch Gesundheitswissenschaften.* Juventa, 1998

[HMMR96] Hennings, Wilfried ; Madjar, Michael ; Mock, Ralf ; Reer, Bernhard: *Aspekte der Risikoanalyse in der verfahrenstechnischen Industrie.* vdf Hochschulverlag AG, 1996

[Hon10] HONGYAN, Wang: *In-depth Road Traffic Accident Research in China.* Automotive College of Tongji University, 2010

[Hör04] HÖRSTE, Michael M.: *Methodische Analyse und generische Modellierung von Eisenbahnleit- und -sicherungssystemen*, TU Braunschweig, Diss., 2004

[HS04] HÄCKER, Hartmut O. ; STAPF, Kurt-H.: *Psychologisches Wörterbuch.* Verlag Hans Huber, 2004

[HS08] HOY, A.W. ; SCHÖNPFLUG, U.: *Pädagogische Psychologie.* Pearson Studium, 2008

[IEC61078] IEC 61078: Analysis techniques for dependability – Reliability block diagram method 1991.

[IEC61508] IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/ programmierbarer elektronischer Systeme / DIN. 2001.

[IEC61882] IEC 61882: Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP) – Leitfaden / IEC. 2001.

[IEC62551] DIN IEC 62551: Analysemethoden für Zuverlässigkeit - Petrinetz-Modellierung / DIN. 2008.

[ISO51] ISO/IEC: Leitfaden für die Aufnahme von Sicherheitsaspekten in Normen / ISO/IEC. 1999.

[ISO15909] ISO/IEC 15909: Software und System-Engineering - Höhere Petri-Netze / ISO. 2004.

[ISO26262] ISO DIS 26262; Road vehicles – Functional safety / ISO. 2008.

[JBAW05] JÄGER, P. ; BERTSCHE, B. ; ARNAOUT, T. ; WUNDERLICH, H.J.: Frühe Zuverlässigkeitsanalyse mechatronischer Systeme. In: *22. Tagung Technische Zuverlässigkeit*, 2005

[Jak02] JAKOBS, Kai: IT-Normen und Standards – Grundlage der Informationsgesellschaft. In: *Die innovative Gesellschaft – Nachfrage für Lead-Märkte von morgen.* BMWI, 2002

[Kau05] KAUBA, Norbert: *Methoden zur Projekt-Priorisierung.* Erfahrungsaustausch Projektmanagement – CSC Deutschland Akademie, 2005

[KCFG04] KLEIN, Torsten ; CONRAD, Mirko ; FEY, Ines ; GROCHTMANN, Matthias: Modellbasierte Entwicklung eingebetteter Fahrzeugsoftware bei DaimlerChrysler. In: *Proceedings Modellierung – Lecture Notes in Informatics (LNI)*, 2004

[KGF07] KAISER, Bernhard ; GRAMLICH, Catharina ; FÖRSTER, Marc: *State-Event Fault Trees – A Safety Analysis Model for Software Controlled Systems.* 2007

[Kis08] KISS, Miklos: Controllability für Lenkeingriffe bei Lenksystemen. In: *Tagungsband der Tagung Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel*, 2008

[KLM03] KAISER, Bernhard ; LIGGESMEYER, Peter ; MÄCKEL, Oliver: A New Component Concept for Fault Trees. In: *SCS*, 2003, S. 37–46

[Kri09] KRISO, Stefan: *Anwendung der ISO 26262 bei Bosch.* 2009. – 6. SafeTRANS Industrial Day

[Lev01] LEVESON, Nancy: *Safeware – System safety and computers.* Eddison Wesley, 2001

[Lig00] LIGGESMEYER, Peter: Formale und stochastische Methoden zur Qualitätssicherung technischer Software. In: *Proceedings Informatik 2000*, 2000

[LL05] LÜDTKE, Andreas ; LEUCHTER, Sandro: Human Error Analyse auf Basis Zweckbestimmter Kognitiver Modelle. In: *WorkshopsProceedings der 5. fachübergreifenden Konferenz Mensch und Computer*, 2005

[LM06] LÜDTKE, Andreas ; MÖBUS, Claus: Human Error Analysis of Safety Critical Systems based on an Integrated Man-Machine Model. In: *7. Bieleschweig Workshop SSystems Engineering": Model-based development and human-centered engineering*, 2006

[Los07] Losano, Mario G.: *Turbulenzen im Rechtssystem der modernen Gesellschaft: Pyramide, Stufenbau und Netzwerkcharakter der Rechtsordnung als ordungsstiftende Modelle.* Duncker+Humblot, 2007

[Lüd04] Lüdtke, Andreas: *Kognitive Analyse Formaler Sicherheitskritischer Steuerungssysteme auf Basis eines integrierten Mensch-Maschine-Modells*, Universität Oldenburg, Diss., 2004

[Mah00] Mahmoud, Rachad: *Sicherheits- und Verfügbarkeitsanalyse komplexer Kfz-Systeme*, Universität-Gesamthochschule Siegen, Diss., 2000

[Mal08] Maldague, Jean-Yves: Nachhaltigkeit: Die entscheidenden Herausforderungen / Dexia. 2008.– Forschungsbericht

[MBKA99] Maria Binfet-Kull, Peter H. ; Ameling, Christian: *Systemsicherheit für ein autonom fahrendes Fahrzeug.* Business Unit, Forschung, Umwelt und Verkehr, 1999

[MBS07] Müller, J.R. ; Becker, U. ; Schnieder, E.: Ergebnisse einer Machbarkeitsstudie zur modellbasierten Diagnose auf Basis von Petrinetzen. In: *Tagungsband zum GMA-Kongress – Automation im gesamten Lebenszyklus.* VDI Wissensforum IWB GmbH, 2007

[Mey00] Meyer, J.-T.: *Simulation.* Vorlesung „Simulation“ an Fachhochschule Nordostniedersachsen, 2000

[MS09] Moser, Andreas ; Steffan, Hermann: Insassensimulation. In: *Handbuch Verkehrsunfallrekonstruktion – Unfallaufnahme, Fahrdynamik, Simulation.* Vieweg+Teubner, 2009

[MSS09] Müller, J.R. ; Ständer, Tobias ; Schnieder, Eckehard: A comparison of safety analysis techniques: Analytical Calculations versus Monte Carlo Simulation. In: *Proceedings ESREL.* European Safety and Reliability Association, 2009

[Noh89] Nohl, J.: *Verfahren zur Sicherheitsanalyse: Eine prospektive Methode zur Analyse und Bewertung von Gefährdungen.* Deutscher Universitäts Verlag, 1989

[OEA09] OEAMTC: *Promillegrenzen in Europa.* http://www.oeamtc.at/../document/touristik/promillegrenze.pdf, 2009. Letzter Aufruf: 08/2010

[OS04] Ostermann, N. ; Schöbel, A.: Zur Sicherheit im Eisenbahnbetrieb / Institut für Eisenbahnwesen, Verkehrswirtschaft und Seilbahnen der TU Wien. 2004. – Forschungsbericht

[Pau07] Paulus, Wilfried: Herleitung der Sicherheitsklasse (ASIL) nach dem Entwurf der „Automobil-Sicherheitsnorm“ ISO 26262 – ein Erfahrungsbericht. In: *Tagungsband zur 27. Tagung Elektronik im Kraftfahrzeug*, 2007

[PBefG61] Bundesministerium für Justiz: *Personenbeförderungsgesetz.* 1961

[PM85] Peters, O.H.; Meyna, A. *Handbuch der Sicherheitstechnik – Band I.* Carl Hanser Verlag, 1985

[Pet62] Petri, Carl A.: *Kommunikation von Automaten*, TH Darmstadt, Diss., 1962

[Pfe01] Pfeifer, Tilo: *Qualitätsmanagement: Strategien, Methoden, Techniken.* Hanser, 2001

[Prä10] Prätorius, Gerhard: *CSR und Nachhaltigkeit als Beitrag zur Reputation des Unternehmens.* http://www.autouni.de/autouni_publish/www/de/lehre, 2010. – Letzter Aufruf: 08/2010

[PS03] Polke, B.; Schnieder, E.: Formalisierte Prozessbeschreibungen – Entwurf der Richtlinie VDI/VDE 3682 und deren Anwendung. In: *atp* 45(2003) Heft 8 , S. 26–33

[Rau08] Rau, Marcus: Development of an Automotive Standard with Focus on Functional Safety (ISO 26262). In: *Proc. World Automotive Congress – FISITA 2008*, 2008

[Red02] Redmill, Felix: Risk analysis – a subjective process. In: *Engineering Management* April (2002)

[Rei85] Reisig, W.: *Systementwurf mit Netzen.* Springer Verlag, 1985

[RH09] Romeike, Frank ; Hager, Peter: *Erfolgsfaktro Risikomanagement 2.0.* Gabler, 2009

[RHE06] Rester, J. ; Hillersheimer, G. ; Engel, J.: *Gütekriterien.* http://www1.abpaed.tu-darmstadt.de/ arbeitsbereiche/bt/ material_ws0607/statistischemethoden/Guetekriterien.pdf, 2006. – letzter Abruf: 08/2010

[70/156/EWG] *Richtlinie des Rates zur Angleichung der Rechtsvorschriften der Mitgliedstatten über die Betriebserlaubnis für Kraftfahrzeuge und Kraftfahrzeuganhänger.* 1970

[2001/95/EG] *Richtlinie des Rates über die allgemeine Produktsicherheit.* 2001

[Rot10] Rothkegel, Annely: *Technikkommunikation.* UTB Stuttgart, 2010

[SBS08] Ständer, Tobias ; Becker, Uwe ; Schnieder, Eckehard: Branchenspezifische Normen und Standards – Aufwand, Nutzen und Herausforderungen. In: *Tagungsband der Tagung Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel*, 2008

[SCEH03] Schnieder, Eckehard ; Chouikha, Mourad ; Einer, Stefan ; Hörste, Michael M.: BASYSNET - An integrated Approach for automated Control System Development. In: *Proceedings - Petri Net Technology for Communication Based Systems.* Springer Berlin, 2003

[Sch92] Schräder, Alfons: *Fach- und Gemeinsprache in der Kraftfahrzeugtechnik – Studien zum Wortschatz.* Lang, 1992

[Sch99a] Schneeweiss, Winfried G.: *Petri Nets for Reliability Modeling.* LiLoLe Verlag GmbH, 1999

[Sch99b] Schnieder, Eckehard: *Methoden der Automatisierung: Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme.* Vieweg, 1999

[Sch03] Schnieder, Eckehard: Beschreibung der Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm. In: *Signal + Draht* 95(10) (2003), S. 6–9

[Sch09] SCHNIEDER, Lars: *Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit*, TU Braunschweig, Diss., 2009

[SCST08] SOLDANI, Sigried ; COMBACAU, Michel ; SUBIAS, Audine ; THOMAS, Jerom: On-board diagnosis system for intermettend fault: Application in automotive industry. In: *Fieldbuses and Networks in Industrial and Embedded Systems,*, 2008

[SEGT05] SCHÖNEBECK, S.; ELLMERS, U. ;GAIL, J. ;TEWS, R. : *Abschätzung möglicher Auswirkungen von Fahren mit Licht am Tag (Tagfahrleuchten / Abblendlicht) in Deutschland.* Bundesanstalt für Straßenwesen – Abschlussbericht, 2005.

[SSP10] STEIN, C.; SCHNIEDER, L.; PFUNDMAYR, M.: Der iglos Terminologie-Engineering-Prozess (iglos tep) zur interdisziplinären und verteilten Terminologiearbeit. In: *EKA 2010 – Entwurf komplexer Automatisierungssysteme 11. Fachtagung*, Magdeburg, 2010

[SSS10] SCHNIEDER, L.; SCHNIEDER, E.; STEIN, C.: Safety and Security; Two sides of the Same Coin: Properties and Relations? Characteristics to refine? Structure of Terminology and its Perception. In: *5th Future Security Conference 2010*, Berlin, 2010

[SL09] STAUBACH, M. ; LÜKEN, P.: Bewertung von Zeugenaussagen verunfallter Fahrzeugführer. In: *Zeitschrift für Verkehrssicherheit* 55 (2009), Nr. 1-4

[Slo06] SLOVAK, Roman: *Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs*, TU Braunschweig, Diss., 2006

[SIA08] SCHWEIZERISCHER INGENIEURSVEREIN: *Die rechtliche Bedeutung der Normen.* http://www.sia.ch/download/normen_bedeutung_d.pdf, 2008. – letzter Abruf: 03/2010

[SPP03] SEIFERT, Tilman ; PIZKA, Markus ; PEISKER, Marcus: Die Bedeutung expliziter Modellierung für die Entwicklung komplexer und langlebiger Software-Systeme / Technische Universität München, BMW Group. Munich, Germany, APR 2003. – internal

[SS09] SCHNIEDER, Lars ; SCHNIEDER, Eckehard: Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung. In: *Sicherheitsforschung – Chancen und Perspektiven.* acatech, 2009

[SSS09] SCHNIEDER, Lars ; SCHNIEDER, Eckehard ; STÄNDER, Tobias: Railway Safety and Security – Two sides of the Same Coin?! In: *Proceedings International Railway Safety Conference*, 2009

[Sta10] STAUBACH, Maria: *Identifikation menschlicher Einflüsse auf Verkehrsunfälle als Grundlage zur Beurteilung von Fahrerassistenzsystem- Potentialen*, TU Dresden, Diss., 2010

[Ste94a] STEINHAUSEN, Detlef: *Simulationstechniken.* Oldenbourg, 1994

[Ste94b] STELZER, Dirk: Risikoanlyse – Konzepte, Methoden und Werkzeuge. In: *Proceedings der Fachtagung SIS*, 1994

[Ste98] STEINSCHADEN, Johannes: *Lehrgang Konstruktionsmethodik.* http://www.staff.fh-vorarlberg.ac.at/hs/Konstruktionsmethodik/Kap_00/KMethod.htm, 1998. – letzter Abruf: 03/2010

[Stö99] STÖCKLI, Reto: *Sozialpsychologische Einflussfaktoren der öffentlichen Risikowahrnehmung von elektromagnetischer Strahlung bei Mobilfunk-Basis-Stationen.* 1999

[Stu07] STURZ, Wolfang: Terminologiemanagement als Fundamet für effektives Wissensmanagement. In: *eDITion* 3 (2007), Nr. 1

[StVZO09] BUNDESGESETZBLATT: *Straßenverkehrs-Zulassungs-Ordnung.* 2009

[SWSB08] STEININGER, Udo ; WEIDL, Thorsten ; STÄNDER, Tobias ; BECKER, Uwe: Der Einsatz einer funktionsorientierten semi-quantitativen Risikoanalyse bei der Entwicklung komplexer Fahrzeugsysteme. In: *Tagungsband der Autoreg*, 2008

[Sys06] SYSKA, Andreas: *Produktionsmanagement: Das A - Z wichtiger Methoden und Konzepte für die Produktion von heute.* Gabler, 2006

[TO02] Thums, A. ; Ortmeier, F.: Formale Methoden und Sicherheitsanalyse / Institut für Informatik der Universität Augsburg. 2002. – Forschungsbericht

[Tro08] Trost, Monika: *Gesamtheitliche Anlagenmodellierung und -analyse auf Basis stochastischer Netzverfahren*, Universität Stuttgart, Diss., 2008

[VDI3681] VDI/VDE 3681: Einordnung und Bewertung von Beschreibungsmitteln aus der Automatisierungstechnik / VDI. 2005.

[VDI3682] VDI/VDE 3682: Formalisierte Prozessbeschreibungen / VDI. 2005.

[VDI4009] VDI 4009 Blatt 10: Analytische Methoden der Fehlererkennung zur Zuverlässigkeitssicherung / VDI. 1986.

[VG01] Voss, Stefan ; Gutenschwager, K.: *Informationsmanagement.* Springer Verlag, 2001

[VGBR10] Vollrath, Mark ; Gelau, Christhard ; Briest, Susanne ; Rataj, Jürgen: Mit Tempomat (zu) entspannt fahren? Eine Simulaturstudie. In: *Tagungsband der Tagung Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel*, 2010

[VH06] Vollrath, Mark ; Hörste, Michael M.: Entwicklung und Bewertung von Automation. Vom Auto zur Bahn und zurück. In: *7. Bieleschweig Workshop SSystems Engineering": Model-based development and human-centered engineering*, 2006

[WBJ00] Watzlawik, Paul ; Beavin, Janet H. ; Jackson, Don D.: *Menschliche Kommunikation – Formen, Störungen, Paradoxien.* Hans Huber, 2000

[WBLS09] Weber, L. ; Baumann, M. ; Lüdtke, A. ; Steenken, R.: Modellierung von Entscheidungen beim Einfädeln auf die Autobahn. In: *Der Mensch im Mittelpunkt technischer Systeme, 8. Berliner Werkstatt, Mensch-Maschine-Systeme*, 2009

[Wer06] Werther, Bernd: *Kognitive Modellierung mit Farbigen Petrinetzen zur Analyse menschlichen Verhaltens*, TU Braunschweig, Diss., 2006

[WHW09] Winner, Hermann ; Hakuli, Stephan ; Wolf, Gabriele: *Handbuch Fahrerassistenzsysteme*. Vieweg+Teubner Verlag, 2009

[WL09] Wortelen, Bertram ; Lüdtke, Andreas: Ablauffähige Modellierung des Einflusses von Ereignishäufigkeiten auf die Aufmerksamkeitsverteilung von Autofahrern. In: *Fortschritt-Berichte VDI, Reihe 21, Nr.29*, 2009

[WML05] Westerkamp, Ralf ; Mrowczynski, Mirdo ; Lamping, Roy: Methods for the Analysis of Safety-Related Functions in Automotive Systems. In: *Tagungsband der Tagung Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel*, 2005

[WW09] Winner, Hermann ; Wolf, Gabriele: Quo vadis, FAS? In: *Handbuch Fahrerassistenzsysteme*. Vieweg+Teubner, 2009

[Zim97] Zimmermann, Armin: *Modellierung und Bewertung von Fertigungssystemen mit Petri-Netzen*, TU Berlin, Diss., 1997

[Zim08] Zimmermann, Armin: RESTART Simulation of Colored Stochastic Petri Nets. In: *International Workshop on Rare Event Simulation*, 2008